frontline
Debug Communications Faster™

User Manual

Revision Date: 11/23/2015

Copyright © 2000-2015 Frontline Test Equipment, Inc.

FTS, Frontline, Frontline Test System, ComProbe Protocol Analysis System and ComProbe are registered trademarks of Frontline Test Equipment, Inc.

The following are trademarks of Frontline Test Equipment, Inc.

- BPA 500

The Bluetooth SIG, Inc. owns the Bluetooth® word mark and logos, and any use of such marks by Frontline is under license. All other trademarks and registered trademarks are property of their respective owners.

Contents

Chapter 1 ComProbe Hardware & Software **1**
1.1 What is in this manual 2
1.2 Computer Minimum System Requirements 2
1.3 Software Installation 2
1.3.1 From CD: 2
1.3.2 From Download: 3
Chapter 2 Getting Started **4**
2.1 BPA 500 Hardware 4
2.1.1 Attaching Antennas 4
2.1.2 Connecting/Powering ComProbe 5
2.1.3 ComProbe BPA 500 LED 6
2.1.4 Connecting for ProbeSync 8
2.2 Data Capture Methods 8
2.2.1 Opening ComProbe Data Capture Method 8
2.2.2 BPA 500 Data Capture Methods 10
2.3 Control Window 11
2.3.1 Control Window Toolbar 12
2.3.2 Configuration Information on the Control Window 13
2.3.3 Status Information on the Control Window 13
2.3.4 Frame Information on the Control Window 13
2.3.5 Control Window Menus 14
2.3.6 Minimizing Windows 17
Chapter 3 Configuration Settings **18**
3.1 BPA 500 Configuration 18
3.1.1 BPA 500 - Update Firmware 18
3.1.2 BPA 500 I/O Settings 19
3.1.2.1 Datasource Toolbar/Menu 19
3.1.2.2 Selecting BPA 500 Devices Under Test 19
3.1.2.3 BPA 500 Devices Under Test 21
3.1.2.3.1 BPA 500 - Devices Under Test - LE Only 21

3.1.2.3.2 BPA 500 - Devices Under Test - Classic Only Single Connection 24
3.1.2.3.3 BPA 500 - Devices Under Test - Dual Mode 26
3.1.2.3.4 BPA 500 - Devices Under Test - Classic Only Multiple Connection 30
3.1.2.3.5 Programmatically Update Link Key from 3rd Party Software 33
3.1.2.4 BPA 500 Device Database 34
3.1.2.5 BPA 500 Information 36
3.1.2.6 BPA 500 Advanced Classic Settings 37
3.2 Decoder Parameters 38
3.2.1 Decoder Parameter Templates 40
3.2.1.1 Select and Apply a Decoder Template 40
3.2.1.2 Adding a New or Saving an Existing Template 41
3.2.1.3 Deleting a Template 41
3.2.2 Selecting A2DP Decoder Parameters 42
3.2.3 AVDTP Decoder Parameters 42
3.2.3.1 About AVDTP Decoder Parameters 42
3.2.3.2 AVDTP Missing Decode Information 44
3.2.3.3 AVDTP Override Decode Information 45
3.2.4 L2CAP Decoder Parameters 47
3.2.4.1 About L2CAP Decoder Parameters 47
3.2.4.2 L2CAP Override Decode Information 48
3.2.5 RFCOMM Decoder Parameters 49
3.2.5.1 About RFCOMM Decoder Parameters 49
3.2.5.2 RFCOMM Missing Decode Information 50
3.2.5.3 RFCOMM Override Decode Information 51
Chapter 4 Capturing and Analyzing Data 53
4.1 Capture Data 53
4.1.1 Air Sniffing: Positioning Devices 53
4.1.2 Capturing Data to Disk - General Procedure 56
4.1.3 Capturing Data with BPA 500 Devices 57
4.1.4 Extended Inquiry Response 60
4.2 Protocol Stacks 60

4.2.1 Protocol Stack Wizard 61
4.2.2 Creating and Removing a Custom Stack 62
4.2.3 Reframing 63
4.2.4 Unframing 63
4.2.5 How the Analyzer Auto-traverses the Protocol Stack 64
4.2.6 Providing Context For Decoding When Frame Information Is Missing 64
4.3 Analyzing Byte Level Data 65
4.3.1 Event Display 65
4.3.2 The Event Display Toolbar 66
4.3.3 Opening Multiple Event Display Windows 68
4.3.4 Calculating CRCs or FCSs 68
4.3.5 Calculating Delta Times and Data Rates 68
4.3.6 Switching Between Live Update and Review Mode 69
4.3.7 Data Formats and Symbols 69
4.3.7.1 Switching Between Viewing All Events and Viewing Data Events 69
4.3.7.2 Switching Between Hex, Decimal, Octal or Binary 70
4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot 71
4.3.7.4 Selecting Mixed Channel/Sides 71
4.3.7.5 List of all Event Symbols 72
4.3.7.6 Font Size 73
4.4 Analyzing Protocol Decodes 74
4.4.1 Frame Display Window 74
4.4.1.1 Frame Display Toolbar 77
4.4.1.2 Frame Display Status Bar 80
4.4.1.3 Hiding and Revealing Protocol Layers in the Frame Display 80
4.4.1.4 Physical vs. Logical Byte Display 81
4.4.1.5 Sorting Frames 81
4.4.1.6 Frame Display - Find 81
4.4.1.7 Synchronizing the Event and Frame Displays 83
4.4.1.8 Working with Multiple Frame Displays 84
4.4.1.9 Working with Panes on Frame Display 84

4.4.1.10 Frame Display - Byte Export 84
4.4.1.11 Panes in the Frame Display 86
4.4.1.11.1 Summary Pane 86
4.4.1.11.2 Customizing Fields in the Summary Pane 89
4.4.1.11.3 Frame Symbols in the Summary Pane 90
4.4.1.11.4 Decode Pane 90
4.4.1.11.5 Radix or Hexadecimal Pane 91
4.4.1.11.6 Character Pane 91
4.4.1.11.7 Binary Pane 92
4.4.1.11.8 Event Pane 92
4.4.1.11.9 Change Text Highlight Color 92
4.4.1.12 Protocol Layer Colors 93
4.4.1.12.1 Data Byte Color Notation 93
4.4.1.12.2 Changing Protocol Layer Colors 93
4.4.1.13 Filtering 93
4.4.1.13.1 Display Filters 94
4.4.1.13.1.5 Defining Node and Conversation Filters
4.4.1.13.1.6 The Difference Between Deleting and Hiding Display Filters
4.4.1.13.1.7 Editing Filters
4.4.1.13.2 Connection Filtering 103
4.4.1.13.2.1 Creating a Connection Filter
4.4.1.13.2.2 Connection Filter Display
4.4.1.13.3 Protocol Filtering from the Frame Display 108
4.4.1.13.3.1 Quick Filtering on a Protocol Layer
4.4.1.13.3.2 Easy Protocol Filtering
4.4.2 Bluetooth Timeline 110
4.4.2.1 Bluetooth Timeline Packet Depiction 111
4.4.2.2 Bluetooth Timeline Packet Navigation and Selection 114
4.4.2.3 Bluetooth Timeline Toolbar 115
4.4.2.4 Bluetooth Timeline Menu Bar 116
4.4.2.5 Bluetooth Timeline Visual Elements 118

4.4.2.6 Bluetooth Timeline Zooming 120
4.4.2.7 Bluetooth Timeline Throughput Displays 120
4.4.2.7.1 Bluetooth Timeline Average Payload Throughput 121
4.4.2.7.2 Bluetooth Timeline 1 Second Throughput Indicators 121
4.4.2.7.3 Average Payload Throughput (bits/s) (Selected) 121
4.4.2.7.4 Bluetooth Payload Throughput Over Time Graph 122
4.4.2.8 Export Payload Throughput Over Time 123
4.4.2.9 Object Throughput Stats File 123
4.4.2.10 Bluetooth Timeline Discontinuities 124
4.4.2.11 Legend 125
4.4.2.12 Bluetooth Timeline: Packets Missing Bluetooth Clock 125
4.4.3 low energy Timeline 126
4.4.3.1 low energy Timeline Toolbar 127
4.4.3.2 low energy Timeline Menu Bar 128
4.4.3.3 low energy Timeline Legend 132
4.4.3.4 Throughput Displays 132
4.4.3.5 Average and 1 Second Packet Throughput 132
4.4.3.6 Average and 1 Second Payload Throughput 132
4.4.3.7 Throughput Graph 132
4.4.3.8 The Timeline 134
4.4.3.9 How Packets Are Displayed 134
4.4.3.10 Format Menu 135
4.4.3.11 low energy Timeline Visual Elements 137
4.4.3.12 low energy Packet Discontinuities 139
4.4.3.13 low energy Timeline Navigating and Selecting Data 140
4.4.3.14 low energy Timeline Zooming 141
4.4.3.15 Zoom menu 142
4.4.3.16 Single Segment Zoom 143
4.4.3.17 Multiple Segments 143
4.4.4 Coexistence View 144
4.4.4.1 Coexistence View - Toolbar 144

4.4.4.2 Coexistence View - Throughput Indicators 146
4.4.4.3 Throughput 146
4.4.4.4 Radio Buttons 147
4.4.4.5 All radio button 147
4.4.4.6 Selected radio button 147
4.4.4.7 Viewport radio button 147
4.4.4.8 Indicator width 148
4.4.4.9 Coexistence View - Throughput Graph 149
4.4.4.10 Throughput Graph Y-axis labels 149
4.4.4.11 Excluded packets 150
4.4.4.12 Tooltips 150
4.4.4.13 Discontinuities 150
4.4.4.14 Viewport 151
4.4.4.15 Swap button 152
4.4.4.16 Dots button 153
4.4.4.17 Zoomed Throughput Graph 154
4.4.4.18 Zoom Cursor 156
4.4.4.19 Comparison with the Bluetooth Timeline's Throughput Graph 156
4.4.4.20 Coexistence View - Set Button 157
4.4.4.21 Coexistence View - Throughput Radio Buttons 158
4.4.4.22 Coexistence View - Timeline Radio Buttons 158
4.4.4.23 Coexistence View – low energy Devices Radio Buttons 158
4.4.4.24 Coexistence View – Legend 159
4.4.4.25 Coexistence View – Timelines 159
4.4.4.26 Packet information 159
4.4.4.27 Relocating the tool tip 162
4.4.4.28 The two Timelines 164
4.4.4.29 Bluetooth slot markers 165
4.4.4.30 Zooming 166
4.4.4.31 Discontinuities 166
4.4.4.32 High-Speed Bluetooth 168

4.4.4.33 Coexistence View - No Packets Displayed with Missing Channel Numbers 168
4.4.4.34 High Speed Live View 169
4.4.5 About The Message Sequence Chart (MSC) 171
4.4.5.1 Message Sequence Chart - Search 175
4.4.5.2 Message Sequence Chart - Go To Frame 176
4.4.5.3 Message Sequence Chart - First Error Frame 177
4.4.5.4 Message Sequence Chart - Printing 177
4.5 Packet Error Rate Statistics 179
4.5.1 Packet Error Rate - Channels (Classic and low energy) 181
4.5.2 Packet Error Rate - Pie Chart and Expanded Chart 183
4.5.3 Packet Error Rate - Legend 184
4.5.4 Packet Error Rate - Additional Statistics 185
4.5.5 Packet Error Rate - Sync Selected Packets With Other Windows 186
4.5.6 Packet Error Rate - Export 186
4.5.7 Packet Error Rate - Scroll Bar 187
4.5.8 Packet Error Rate - Excluded Packets 189
4.6 Data/Audio Extraction 190
Chapter 5 Navigating and Searching the Data 193
5.1 Find 193
5.1.1 Searching within Decodes 194
5.1.2 Searching by Pattern 196
5.1.3 Searching by Time 198
5.1.4 Using Go To 200
5.1.5 Searching for Special Events 201
5.1.6 Searching by Signal 202
5.1.7 Searching for Data Errors 206
5.1.8 Find - Bookmarks 208
5.1.9 Changing Where the Search Lands 209
5.1.10 Subtleties of Timestamp Searching 210
5.2 Bookmarks 210
5.2.1 Adding, Modifying or Deleting a Bookmark 210

5.2.2 Displaying All and Moving Between Bookmarks 211
Chapter 6 Saving and Importing Data 213
6.1 Saving Your Data 213
6.1.1 Saving the Entire Capture File 213
6.1.2 Saving the Entire Capture File with Save Selection 214
6.1.3 Saving a Portion of a Capture File 215
6.2 Adding Comments to a Capture File 215
6.3 Confirm Capture File (CFA) Changes 216
6.4 Loading and Importing a Capture File 216
6.4.1 Loading a Capture File 216
6.4.2 Importing Capture Files 217
6.5 Printing 217
6.5.1 Printing from the Frame Display/HTML Export 217
6.5.2 Printing from the Event Display 219
6.6 Exporting 220
6.6.1 Frame Display Export 220
6.6.2 Exporting a File with Event Display Export 221
6.6.2.1 Export Filter Out 223
6.6.2.2 Exporting Baudot 223
Chapter 7 General Information 224
7.1 System Settings and Progam Options 224
7.1.1 System Settings 224
7.1.1.1 System Settings - Disabled/Enabled Options 226
7.1.1.2 Advanced System Options 226
7.1.1.3 Selecting Start Up Options 227
7.1.2 Changing Default File Locations 228
7.1.3 Side Names 230
7.1.4 Timestamping 231
7.1.4.1 Timestamping Options 231
7.1.4.2 Enabling/Disabling Timestamp 232
7.1.4.3 Changing the Timestamp Resolution 232

7.1.4.4 Switching Between Relative and Absolute Time 233
7.1.4.5 Displaying Fractions of a Second 234
7.2 Technical Information 234
7.2.1 Performance Notes 234
7.2.2 BTSnoop File Format 235
7.2.3 Ring Indicator 237
7.2.4 Progress Bars 238
7.2.5 Event Numbering 238
7.2.6 Useful Character Tables 238
7.2.6.1 ASCII Codes 238
7.2.6.2 Baudot Codes 239
7.2.6.3 EBCDIC Codes 239
7.2.6.4 Communication Control Characters 239
7.2.7 The Frontline Serial Driver 241
7.2.8 DecoderScript Overview 241
7.2.9 Bluetooth low energy ATT Decoder Handle Mapping 242
7.3 Contacting Technical Support 243
Appendicies 244
Appendix A: Application Notes 246
A.1 Getting the Android Link Key for Classic Decryption 248
A.1.1 What You Need to Get the Android Link Key 248
A.1.2 Activating Developer options 248
A.1.3 Retrieving the HCI Log 249
A.1.4 Using the ComProbe Software to Get the Link Key 250
A.2 Decrypting Encrypted Bluetooth®data with ComProbe BPA 600 254
A.2.1 How Encryption Works in Bluetooth 254
A.2.2 Legacy Pairing (Bluetooth 2.0 and earlier) 254
A.2.3 Secure Simple Pairing (SSP) (Bluetooth 2.1 and later) 256
A.2.4 How to Capture and Decrypt Data (Legacy Pairing) 256
A.2.5 How to tell if a device is in Secure Simple Pairing Debug Mode 258
A.3 Decrypting Encrypted Bluetooth® low energy 262

A.3.1 How Encryption Works in Bluetooth low energy 262
A.3.2 Pairing 262
A.3.3 Pairing Methods 263
A.3.4 Encrypting the Link 264
A.3.5 Encryption Key Generation and Distribution 264
A.3.6 Encrypting The Data Transmission 265
A.3.7 Decrypting Encrypted Data Using ComProbe BPA 600 low energy Capture 265
A.4 Bluetooth® low energy Security 272
A.4.1 How Encryption Works in Bluetooth low energy 273
A.4.2 Pairing 273
A.4.3 Pairing Methods 274
A.4.4 Encrypting the Link 275
A.4.5 Encryption Key Generation and Distribution 275
A.4.6 Encrypting The Data Transmission 276
A.4.7 IRK and CSRK Revisited 276
A.4.8 Table of Acronyms 277
A.5 Bluetooth Virtual Sniffing 278
A.5.1 Introduction 278
A.5.2 Why HCI Sniffing and Virtual Sniffing are Useful 278
A.5.3 Bluetooth Sniffing History 279
A.5.4 Virtual Sniffing—What is it? 279
A.5.5 The Convenience and Reliability of Virtual Sniffing 280
A.5.6 How Virtual Sniffing Works 280
A.5.7 Virtual Sniffing and Bluetooth Stack Vendors 280
A.5.8 Case Studies: Virtual Sniffing and Bluetooth Mobile Phone Makers 281
A.5.9 Virtual Sniffing and You 281

List of Figures

Figure 2.1 - Front Panel 4
Figure 2.2 - ComProbe BPA 500 with antennas attached. 5

Figure 2.3 - Back Panel - Power 5
Figure 2.4 - Back Panel - USB 6
Figure 2.5 - BPA 500 Front Panel LEDs 7
Figure 2.6 - Desktop Folder Link 9
Figure 2.7 - ComProbe Analyzer Control Window 11
Figure 3.1 - Select Set Initial Decoder Parameters... from Control window 39
Figure 3.2 - Tabs for each decoder requiring parameters. 39
Figure 3.3 - Set Subsequent Decoder Parameters... from Control window 40
Figure 3.4 - Example: Set Subsequent Decode for Frame #52, RFCOMM 40
Figure 3.5 - A2DP Decoder Settings 42
Figure 3.6 - AVDTP parameters tab 43
Figure 3.7 - Parameters Added to Decoder 43
Figure 3.8 - Look in Decoder pane for profile hints 44
Figure 3.9 - AVDTP Override of Frame Information, Item to Carry 46
Figure 3.10 - AVDTP Override of Frame Information, Media Codec Selection 46
Figure 3.11 - L2CAP Decoder parameters tab 47
Figure 3.12 - Parameters Added to Decoder 48
Figure 3.13 - RFCOMM parameters tab 49
Figure 3.14 - Parameters Added to Decoder 50
Figure 3.15 - Set Subsequent Decoder Parameters selection list 52
Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane 54
Figure 4.2 - For Audio A2DP, Position Closer to SINK DUT 55
Figure 4.3 - Example: Poor Capture Environment 56
Figure 4.4 - Packet Transfer Dialog 57
Figure 4.5 - BPA 500 Datasource Dialog 58
Figure 4.6 - Frame Display Extended Inquire Response 60
Figure 4.7 - Format Menu 70
Figure 4.8 - Header labels, right click 70
Figure 4.9 - Data display right click menu 71
Figure 4.10 - Event Display Options menu 74
Figure 4.11 - Event Display Font Size Selection 74

Figure 4.12 - Frame Display with all panes active 75
Figure 4.13 - Frame Display Find text entry field 81
Figure 4.14 - Search/Find Dialog 82
Figure 4.15 - Frame Display File menu, Byte Export 85
Figure 4.16 - Byte Export dialog 85
Figure 4.17 - Save As dialog 86
Figure 4.18 - Sample Exported Frames Text File 86
Figure 4.19 - Example Protocol Tags 87
Figure 4.20 - Summary pane (right) with Tooltip on Column 5 (Tran ID) 88
Figure 4.21 - Frame Display Protocol Layer Color Selector 93
Figure 4.22 - Example: Set Conditions Self Configuring Based on Protocol Selection 95
Figure 4.23 - Example: Set Conditions Self Configuring Based on Frame Range 96
Figure 4.24 - Two Filter Conditions Added with an AND Operator 98
Figure 4.25 - Save Named Filter Condition Dialog 98
Figure 4.26 - Using Named Filters Section of Quick Filters to Show/Hide Filters 101
Figure 4.27 - Set Condition Dialog in Advanced View 102
Figure 4.28 - Rename Filters Dialog 103
Figure 4.29 - Connection Filter from the Frame Display Menu 104
Figure 4.30 - Connection Filter from the Frame Display Toolbar right-click 104
Figure 4.31 - Connection Filter from the Frame Display Pane right-click 105
Figure 4.32 - Connection Filter from frame selection right-click 106
Figure 4.33 - Front Display: Filtered on Access Address 0x8e89bed6 107
Figure 4.34 - Unfiltered: Capture File with Classic, low energy, and 802.11 108
Figure 4.35 - Connection Filter selecting All 802.11 frames, front 108
Figure 4.36 - Frame Display Quick Filtering and Hiding Protocols Dialog 109
Figure 4.37 - Bluetooth Timeline window 110
Figure 4.38 - Bluetooth Timeline Packet Depiction with Packet Information Shown 111
Figure 4.39 - Missing packets message in timeline pane. 126
Figure 4.40 - Bluetooth low energy Timeline 126
Figure 4.41 - Bluetooth low energy Timeline Throughput Graph 133
Figure 4.42 - Creating Encrypted MIC in Frame Display Summary pane 134

Figure 4.43 - Bluetoothlow energy Timeline 134
Figure 4.44 - Diagram of low energy Timeline Flow with Segment and Row Relationship 135
Figure 4.45 - Device Address Rows 136
Figure 4.46 - Radio Rows 136
Figure 4.47 - low energy Timeline and Frame Display Packet Synchronization 137
Figure 4.48 - Timeline Markers Shown Snapped to End of Packet 137
Figure 4.49 - Bluetooth le Timeline Segment Timestamp and Zoom Value 138
Figure 4.50 - Bluetooth le Timeline Packet Info Line 138
Figure 4.51 - Bluetooth le Timeline Packet Info Line for Multiple Selected Packets 139
Figure 4.52 - Bluetooth® low energy Packet Discontinuity 139
Figure 4.53 - low energy Timeline Zoom menu 142
Figure 4.54 - Coexistence View Window 144
Figure 4.55 - Coexistence View Toolbar 144
Figure 4.56 - Coexistence View Throughput Indicators 146
Figure 4.57 - Throughput Graph viewport. 148
Figure 4.58 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded. 148
Figure 4.59 - A single selected packet 148
Figure 4.60 - Coexistence View Throughput Graph 149
Figure 4.61 - Throughput Graph y-axis labels. 150
Figure 4.62 - Data point tooltip 150
Figure 4.63 - A negative discontinuity. 151
Figure 4.64 - Three positive discontinuities. 151
Figure 4.65 - Throughput Graph Viewport 152
Figure 4.66 - Small Timeline and large Throughput Graph after pressing the Swap button. 153
Figure 4.67 - Dots Toggled On and Off 153
Figure 4.68 - Overlapping Dots Information Display 154
Figure 4.69 - Synchronized Zoomed Throughput Graph and View Port 155
Figure 4.70 - Zoomed Throughput Graph- Largest Value Snaps to Top 155
Figure 4.71 - Zoomed Throughput Graph - Freeze Y keeps the y-axis constant 156
Figure 4.72 - 802.11 Source Address Dialog 157
Figure 4.73 - 802.11 Source Address Drop Down Selector 158

Figure 4.74 - Coexistence View Legend 159
Figure 4.75 - Coexistence View Timelines 159
Figure 4.76 - Each packet is color-coded 160
Figure 4.77 - Highlighted entries in the legend for a selected packet. 160
Figure 4.78 - Timeline header for a single selected packet. 160
Figure 4.79 - Timeline header for multiple selected packets 161
Figure 4.80 - Descriptive text on timeline packets. 161
Figure 4.81 - A tool tip for a Classic Bluetooth packet. 162
Figure 4.82 - Coexistence View Format Menu - Show Tooltips on Computer Screen 163
Figure 4.83 - Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen 164
Figure 4.84 - 5 GHz and 2.4 GHz 802.11 packets 164
Figure 4.85 - 5 GHz information window 165
Figure 4.86 - 2.4 GHz information windows 165
Figure 4.87 - Vertical blue lines are Bluetooth slot markers 166
Figure 4.88 - A negative discontinuity 167
Figure 4.89 - A positive discontinuity 167
Figure 4.90 - Timeline header with discontinuity 167
Figure 4.91 - Timeline duration footer with discontinuity 167
Figure 4.92 - High-speed Bluetooth packets have a blue frequency box and a two-tone tool tip 168
Figure 4.93 - Missing Channel Numbers Message in Timelines 169
Figure 4.94 - Message Sequence Chart Window 171
Figure 4.95 - Classic and LE tabs 172
Figure 4.96 - Frame# and Time Display, inside red box. 173
Figure 4.97 - MSC Synchronization with Frame Display 173
Figure 4.98 - Control and Signaling Frames Summay 174
Figure 4.99 - Packet Layers Shown in Different Colors 174
Figure 4.100 - Right-Click in Ctrl Summary to Display Show in MSC 174
Figure 4.101 - MSC View of Selected Packet from Ctrl Summary 175
Figure 4.102 - Return to Text View Using Right-Click Menu 175
Figure 4.103 - Highlighted First Search Result 176
Figure 4.104 - Message Sequence Chart Print Preview 178

Figure 4.105 - Print Preview Toolbar 178
Figure 4.106 - Classic Bluetooth PER Stats Window 180
Figure 4.107 - Bluetooth low energy PER Stats Window 181
Figure 4.108 - Classic Bluetooth Packet Error Rate Channels 182
Figure 4.109 - Bluetooth low energy Packet Error Rate Channels 182
Figure 4.110 - Save As dialog in PER Stats Export 187
Figure 4.111 - PER Stats Scroll Bar 187
Figure 4.112 - Example: Excluded Packets Message in Scroll Bar (Classic Bluetooth) 190
Figure 5.1 - Find Dialog 193
Figure 5.2 - Find Decode Tab Search for String 194
Figure 5.3 - Find Decode Tab Side Restriction 195
Figure 5.4 - Find Pattern Tab 197
Figure 5.5 - Find Pattern Tab Side Restrictions 197
Figure 5.6 - Find by Time tab 198
Figure 5.7 - Find Go To tab 200
Figure 5.8 - Find Special Events tab 202
Figure 5.9 - Find Signal tab. 203
Figure 5.10 - Find Signal Tab 204
Figure 5.11 - Find Error tab. 206
Figure 5.12 - Find Bookmark tab. 209
Figure 5.13 - Bookmarked Frame (3) in the Frame Display 210
Figure 5.14 - Find Window Bookmark tab Used to Move Around With Bookmarks 212
Figure 6.1 - Windows Save dialog 214
Figure 6.2 - Frame Display Print Dialog 218
Figure 6.3 - Frame Display Print Preview Dialog 219
Figure 6.4 - Event Display Print Dialog 220
Figure 6.5 - Event Display Export Example: .csv file. 221
Figure 6.6 - Example: .csv Event Display Export, Excel spreadsheet 223
Figure 7.1 - System Settings Single File Mode 225
Figure 7.2 - Advanced System Options dialog 227
Figure 7.3 - Start Up Options dialog 228

Figure 7.4 - File Locations dialog 229
Figure 7.5 - File Locations Browse dialog 229
Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current 231

Chapter 1 ComProbe Hardware & Software

Frontline Test Equipment ComProbe family of protocol analyzers work with the following technologies.

- Classic Bluetooth®
- *Bluetooth* low energy
- Dual Mode *Bluetooth* (simultaneous Classic and low energy)
- *Bluetooth* Coexistence with 802.11
- *Bluetooth* HCI (USB, SD, High Speed UART)
- NFC
- 802.11 (Wi-Fi)
- SD
- USB
- HSU (High Speed UART)

The ComProbe hardware interfaces with your computer that is running our robust software engine called the ComProbe Protocol Analysis System or ComProbe software. Whether you are sniffing the air or connecting directly to the chip Frontline analyzers use the same powerful ComProbe software to help you test, troubleshoot, and debug communications faster.

ComProbe software is an easy to use and powerful protocol analysis platform. Simply use the appropriate ComProbe hardware or write your own proprietary code to pump communication streams directly into the ComProbe software where they are decoded, decrypted, and analyzed. Within the ComProbe software you see packets, frames, events, coexistence, binary, hex, radix, statistics, errors, and much more.

This manual is a user guide that takes you from connecting and setting up the hardware through all of the ComProbe software functions for your ComProbe hardware. Should you have any questions contact the Frontline Technical Support Team.

1.1 What is in this manual

The ComProbe User Manual comprises the following seven chapters. The chapters are organized in the sequence you would normally follow to capture and analyze data: set up, configure, capture, analyze, save. You can read them from beginning to end to gain a complete understanding of how to use the ComProbe hardware and software or you can skip around if you only need a refresher on a particular topic. Use the Contents, Index, and Glossary to find the location of particular topics.

- **Chapter 1 ComProbe Hardware and Software**. This chapter will describe the minimum computer requirements and how to install the software.
- **Chapter 2 Getting Started**. Here we describe how to set up and connect the hardware, and how to apply power. This chapter also describes how to start the ComProbe software in Data Capture Methods. You will be introduced to the Control window that is the primary operating dialog in the ComProbe software.
- **Chapter 3 Configuration Settings**. The software and hardware is configured to capture data. Configuration settings may vary for a particular ComProbe analyzer depending on the technology and network being sniffed. There are topics on configuring protocol decoders used to disassemble packets into frames and events.
- **Chapter 4 Capturing and Analyzing Data**. This Chapter describes how to start a capture session and how to observe the captured packets, frames, layers and events.
- **Chapter 5 Navigating and Searching the Data**. Here you will find how to move through the data and how to isolate the data to specific events, often used for troubleshooting device design problems.
- **Chapter 6 Saving and Importing Data**. When a live capture is completed you may want to save the captured data for future analysis, or you may want to import a captured data set from another developer or for use in interoperability testing. This chapter will explain how to do this for various data file formats.
- **Chapter 7 General Information**. This chapter provides advanced system set up and configuration information, timestamping information, and general reference information such as ASCII, baudot, and EBCDIC codes. This chapter also provides information on how to contact Frontline's Technical Support team should you need assistance.

1.2 Computer Minimum System Requirements

Frontline supports the following computer systems configurations:

- Operating System: Windows 7 and 8
- USB Port: USB 2.0 or USB 3.0 High-Speed

The ComProbe software must operate on a computer with the following minimum characteristics.

- Processor: Core i5 processor at 2.7 GHz
- RAM: 4 GB
- Free Hard Disk Space: 20 GB

1.3 Software Installation

1.3.1 From CD:

Insert the ComProbe installer disc into your DVD drive. Click on the **Install CPAS** shortcut and follow the directions.

1.3.2 From Download:

Download the latest **CPAS installer** from FTE.com. Once downloaded, double-click the installer and follow the directions.

Chapter 2 Getting Started

In this chapter we introduce you to the ComProbe hardware and show how to start the ComProbe analyzer software and explain the basic software controls and features for conducting the protocol analysis.

2.1 BPA 500 Hardware

The following sections describe the ComProbe BPA 500 hardware connectors and hardware setup. the BPA 500 analyzer is a Frontline legacy product no longer manufactured or sold. This section is provided for those users still using the BPA 500 protocol analysis system. The BPA 600 protocol analyzer is a replacement for the BPA 500 analyzer.

2.1.1 Attaching Antennas

When you remove the ComProbe from the box, the first step is to attach the antennas (Figure 2.1).

Figure 2.1 - Front Panel

1. Attach antennas to RF under LE and RF under CLASSIC.

Figure 2.2 - ComProbe BPA 500 with antennas attached.

2.1.2 Connecting/Powering ComProbe

Once you have attached the antennas, the next step is to power up and connect the ComProbe BPA 500 to the computer.

1. Insert the power cable (DC connector) from the 12 volt AC adapter into the "Power" port on the ComProbe (Figure 2.3).

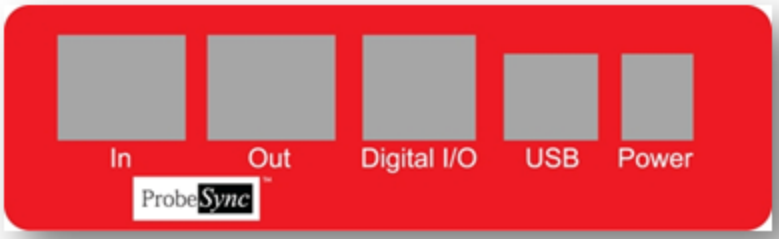


Figure 2.3 - Back Panel - Power

2. Plug the 12 volt AC adapter into the AC power source.

AC Adapter Details:

ECOPAC (UK) POWER LTD, Switch Mode Power Supply –

Model: 3A-181WP09

P/N: T3508ST

Input: 100-240V~, 50-60Hz, 0.6A

Output: +9V-2.0A

3. Insert the USB cable into the USB port on the ComProbe (Figure 2.4).

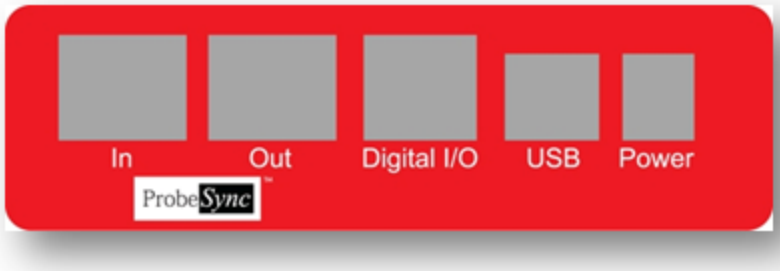


Figure 2.4 - Back Panel - USB

Note: The ComProbe WILL NOT function properly when only the USB is plugged in. The AC power must also be connected.

4. Insert the other end of the USB cable into the PC.
5. Turn on the devices that you are testing.
6. Finally position the BPA 500 between the devices.

   It may be easier to sync and then capture data if the devices are somewhat separated because Bluetooth adjusts power levels on devices that are in close proximity, which can affect the ability to sync and the quality of the trace. Also, don't place the BPA 500 right next to the computer; close proximity to the computer could cause some interference.

2.1.3 ComProbe BPA 500 LED

The BPA 500 has seven LEDs on the RF panel. In the center are the **Ready** and **External Clock** green LEDs. When the **Ready** LED is illuminated the device has booted and is prepared to begin receiving signals for processing. The **External Clock**, when illuminated, indicates that the device is actively using the external clock.

Figure 2.5 - BPA 500 Front Panel LEDs

LE Section

The **LE** (low energy) RF section of the panel has three blue LEDs: **Sync 1**, **2**, and **3**, one for each Bluetooth® LE radio chip. The behavior of each LED is as follows:

Table 2.1 - ComProbe BPA 500 Capture LED Status _ Low Energy

LED Color	BPA 500 Status
LED Off	Sniffing low energy advertising traffic, or sniffing has not started.
Steady Blue	Capturing data from a low energy data connection. Since the connection events in a data connection are fairly short, the LED will be on for a short time and thus appear to flash on briefly and then off again. When sniffing a single connection the frequency with which the LED flashes represents the duration of the connection interval.
Flash Blue *(The LED will regularly alternate between blue and off with a frequency of about 4 times a second.)*	The sniffer is capturing ID packets. That is, the master device is paging the slave, but the connection is not yet established. When the connection gets established it will be followed by a Classic LED and thus the LE LED is off.

Classic Section

The **Classic** RF section of the panel has two tri-colored LEDs: **Sync 1** and **2**, one for each Classic *Bluetooth* radio chip. The behavior of each LED is as follows.

Table 2.2 - ComProbe BPA 500 Capture LED Status - Classic Bluetooth

LED Color	BPA 500 Status
LED Off	Out of lock when sniffing a Classic connection, or sniffing has not started.

Table 2.2 - ComProbe BPA 500 Capture LED Status - Classic Bluetooth (continued)

LED Color	BPA 500 Status
Steady Yellow	Sniffer is ready to capture the master connecting to the slave
Flash Blue/Yellow *(Regularly alternating between yellow and blue with a frequency of about 4 times a second.)*	Sniffer is capturing the master paging the slave, but the connection has not been established yet.
Steady Blue	Sniffing Classic connection and locked.
Flash Pink *(Regularly alternating between a pale pink and off with a frequency of about 6 times a second.)*	Classic connection has terminated and sniffer is in Alternate mode. The sniffer will only be able to follow a reconnection for a short period in this state and will thus resync quickly.

2.1.4 Connecting for ProbeSync

Any ComProbe analyzer with ProbeSync can be connected together to run off of a common clock, ensuring that the timestamps are precisely synchronized between the sniffing hardware.

Simply plug the supplied Cat 5 cable into the OUT connector on the sniffer that will be supplying the clock (the master) and connect the other end to the IN connector on the sniffer to be sharing the master's clock (the slave). If more than two ComProbe devices or BPA 500 hardware are used, just connect the OUT connector from the first slave to the second slave IN connector. If a BPA 500 hardware is being used with another ComProbe device, the BPA 500 hardware must be the master. The combined length of all the ProbeSync cables connected at a given time should not exceed 1.5 meters (4.5 feet).

2.2 Data Capture Methods

This section describes how to load Frontline Test Equipment, Inc ComProbe Protocol Analysis System software, and how to select the data capture method for your specific application.

2.2.1 Opening ComProbe Data Capture Method

On product installation, the installer creates a folder on the windows desktop labeled "Frontline ComProbe Protocol Analysis System <version#>".

1. Double-click the "Frontline ComProbe Protocol Analysis System" desktop folder

This opens a standard Windows file folder window.

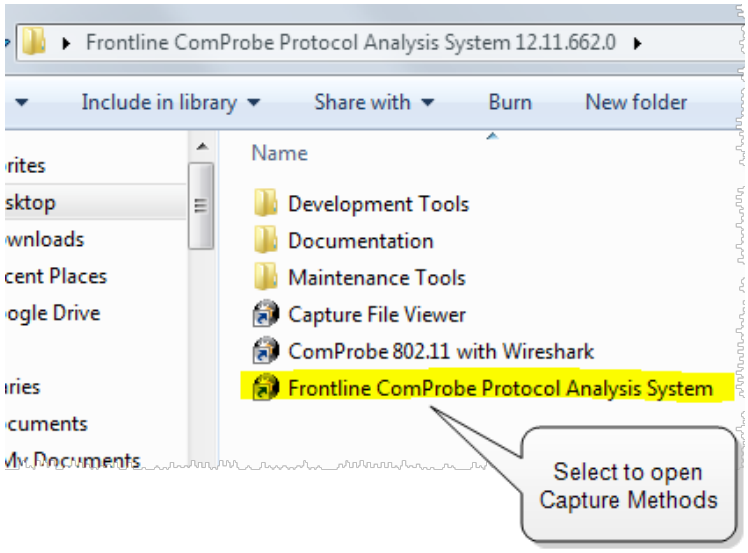


Figure 2.6 - Desktop Folder Link

2. Double-click on **Frontline ComProbe Protocol Analysis System** and the system displays the Select Data Capture Method dialog.

Note: You can also access this dialog by selecting Start > All Programs > Frontline ComProbe Protocol Analysis System (Version #) > Frontline ComProbe Protocol Analysis System

Three buttons appear at the bottom of the dialog; **Run**, **Cancel**, and **Help**. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).

Run starts the selected protocol stack.

Cancel closes the dialog and exits the user back to the desktop.

Help takes the user to this help file as does pressing the F1 key.

3. Expand the folder and select the data capture method that matches your configuration.
4. Click on the Run button and the ComProbe Control Window will open configured to the selected capture method.

Note: If you don't need to identify a capture method, then click the Run button to start the analyzer.

Creating a Shortcut

A checkbox labeled Create Shortcut When Run is located near the bottom of the dialog. This box is un-checked by default. Select this checkbox, and the system creates a shortcut for the selected method, and places it in the "Frontline ComProbe Protocol Analysis System <version#>" desktop folder and in the start menu when you click

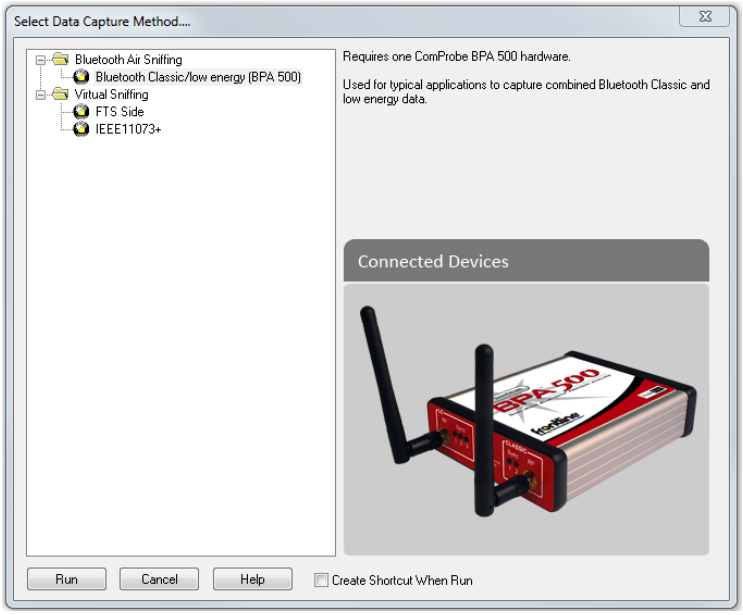
the Run button. This function allows you the option to create a shortcut icon that can be placed on the desktop. In the future, simply double-click the shortcut to start the analyzer in the associated protocol.

Supporting Documentation

The Frontline ComProbe Protocol Analysis System directory contains supporting documentation for development (Automation, DecoderScript, application notes), user documentation (Quick Start Guides and User Manual), and maintenance tools.

2.2.2 BPA 500 Data Capture Methods

ComProbe® Protocol Analysis System has different data capture methods to accommodate various applications.



- **BR/EDR - low energy Air Sniffing**
  - This method requires one BPA 500 ComProbe and is used to capture combined BR/EDR and Bluetooth® low energy data.
  - Used for typical applications to capture Classic *Bluetooth* and *Bluetooth* low energy data.
  - Modes include:
    - LE Only - *Bluetooth* low energy only
    - Classic Only Single Connection
    - Dual Mode - Classic *Bluetooth* and Bluetooth low energy.
    - Classic Only Multiple Connections

- **Classic/low energy/802.11 Air Sniffing (optional)**
- **Two 802.11 and One BPA500**
  - This method requires one BPA 500 ComProbe and two ComProbe 802.11 hardware.
  - An 802.11 ComProbe hardware is included with the Wi-Fi Option.
  - Used for Bluetooth Classic/low energy/802.11 coexistence analysis.
  - Captures Bluetooth Classic, low energy, and 802.11 data and displays in the Frame Display and Coexistence View.
- **802.11/Classic/low energy Coexistence**
  - This method requires one ComProbe BPA500 and one ComProbe 802.11 hardware.
  - Captures Bluetooth Classic, low energy, and 802.11 data and displays in the Frame Display and Coexistence View.

2.3 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The Control window opens when the **Run** button is clicked in the **Select Data Capture Method** window. The Control window provides access to each ComProbe analyzer functions and settings as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function. A sample Control Window is shown below.

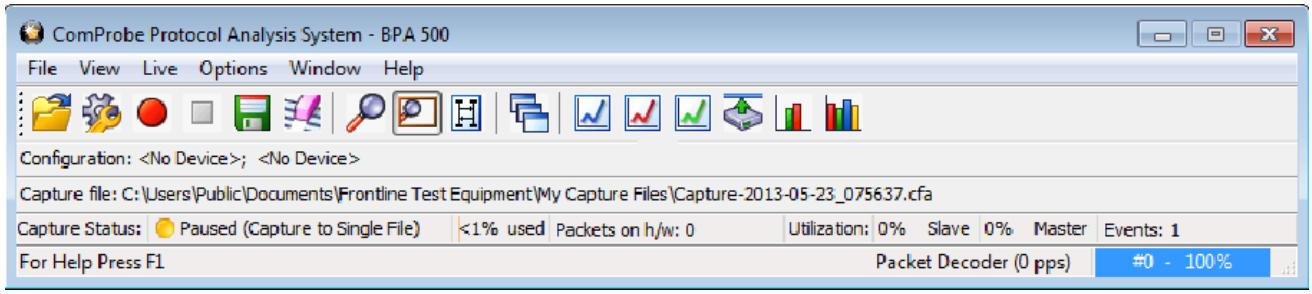

ComProbe Protocol Analysis System - BPA 500
File View Live Options Window Help
Configuration: <No Device>; <No Device>
Capture file: C:\Users\Public\Documents\Frontline Test Equipment\My Capture Files\Capture-2013-05-23_075637.cfa
Capture Status: Paused (Capture to Single File) <1% used Packets on h/w: 0 Utilization: 0% Slave 0% Master Events: 1
For Help Press F1 Packet Decoder (0 pps) #0 - 100%

Figure 2.7 - ComProbe Analyzer Control Window

Because the **Control** window can get lost behind other windows, every window has a **Home** icon that brings the Control window back to the front. Just click on the Home icon to restore the **Control** window.

When running the Capture File Viewer, the Control window toolbar and menus contain only those selections needed to open a capture file and display the About box. Once a capture file is opened, the analyzer limits Control window functions to those that are useful for analyzing data contained in the current file. Because you cannot capture data while using Capture File Viewer, data capture functions are unavailable. For example, when viewing Ethernet data, the Signal Display is not available. The title bar of the Control window displays the name of the currently open file. The status line (below the toolbar) shows the configuration settings that were in use when the capture file was created.

2.3.1 Control Window Toolbar

Toolbar icon displays vary according to operating mode and/or data displayed. Available icons appear in color, while unavailable icons are not visible. Grayed-out icons are available for the ComProbe hardware and software configuration in use but are not active until certain operating conditions occur. All toolbar icons have corresponding menu bar items or options.

Table 2.3 - Control Window Toolbar Icon List

Icon	Description
	Open File - Opens a capture file.
	I/O Settings - Opens settings
	Start Capture - Begins data capture to disk
	Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.
	Save - Saves the capture file.
	Clear - Clears or saves the capture file.
	Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.
	Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.
	Notes - Opens the Notes dialog.
	Cascade - Arranges windows in a cascaded display.
	Bluetooth Packet Timeline - Opens the Packet Timeline dialog.
	Coexistence View - Opens the Coexistence View dialog.
	Low energy - Opens the low energy Timeline dialog.
	Extract Data/Audio - Opens the Extract Data/Audio dialog.
	MSC Chart - Opens the Message Sequence Chart
	Bluetooth low energy Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.
	Bluetooth Classic Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.

2.3.2 Configuration Information on the Control Window

The Configuration bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc.

2.3.3 Status Information on the Control Window

The Status bar located just below the Configuration bar on the **Control** window provides a quick look at current activity in the analyzer.

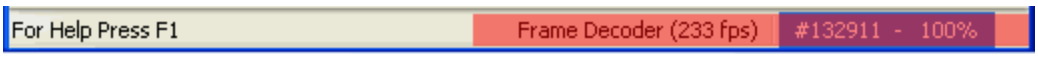
- Capture Status, or Status for Sodera, displays Not Active, Paused or Running and refers to the state of data capture
    - Not Active means that the analyzer is not currently capturing data.
    - Paused means that data capture has been suspended.
    - Running means that the analyzer is actively capturing data.
- % Used

    The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200 Kb capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to overwrite the oldest data, depending on the choices you made in the System Settings.
- Utilization/Events

    The second half of the status bar gives the current utilization and total number of events seen on the network. This is the total number of events monitored, not the total number of events captured. The analyzer is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.

2.3.4 Frame Information on the Control Window

Frame Decoder information is located just below the Status bar on the Control window. It displays two pieces of information.



- Frame Decoder (233 fps) displays the number of frames per second being decoded. You can toggle this display on/off with Ctrl-D, but it is available only during a live capture.
- #132911 displays the total frames decoded.

- 100% displays the percentage of buffer space used.

2.3.5 Control Window Menus

The menus appearing on the **Control** window vary depending on whether the data is being captured live or whether you are looking at a .cfa file. The following tables describe each menu.

Table 2.4 - Control Window **File** Menu Selections

Mode	Selection	Hot Key	Description
Live	**Close**		Closes Live mode.
Capture File	**Go Live**		Returns to Live mode
	Reframe		If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. See Reframing on page 63
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 63
	Recreate Companion File		This option is available when you are working with decoders. If you change a decoder while working with data, you can recreate the ".frm file", the companion file to the ".cfa file". Recreating the ".frm file" helps ensure that the decoders will work properly.
	Reload Decoders		The plug-ins are reset and received frames are decoded again.
Live & Capture File	**Open Capture File**	Ctrl--O	Opens a Windows Open file dialog. at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\". Capture files have a .cfa extension.
	Save	Ctrl-S	Saves the current capture or capture file. Opens a Windows Save As dialog at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\".
	Exit ComProbe Protocol Analysis System		Shuts down the ComProbe Protocol Analysis System and all open system windows.
	Recent capture files		A list of recently opened capture files will appear.

The **View** menu selections will vary depending on the ComProbe analyzer in use.

Table 2.5 - Control Window **View** Menu Selections

Mode	Selection	Hot key	Description
Live & Capture File	**Event Display**	Ctrl-Shift-E	Opens the Event Display window for analyzing byte level data.
	Frame Display	Ctrl-Shift-M	Opens the Frame Display window for analyzing protocol level data
	Bluetooth Timeline		Opens the Bluetooth Timeline window for analyzing protocol level data in a packet chronological format and in packet throughput graph.
	Coexistence View		Opens the Coexistence View window that can simultaneously display Classic *Bluetooth*, *Bluetooth* low energy, and 802.11 packets and thourghput.
	Bluetooth low energy Timeline		Opens the Bluetooth low energy Timeline window for analyzing protocol level data in a packet chronological format and in packet throughput graph.
	Extract Data Audio...		Opens the Data/Audio Extraction dialog for pulling data from decoded *Bluetooth* protocols.
	Bluetooth low energy Packet Error Rate Statistics		Opens the *Bluetooth* low energy PER Stats window to show a dynamic graphical representation of the error rate for each low energy channel.
	Classic Bluetooth Packet Error Rate Statistics		Opens the Classic *Bluetooth* PER Stats window to show a dynamic graphical representation of the error rate for each channel.

Table 2.6 - Control Window **Edit** Menu Selections

Mode	Selection	Hot-key	Description
Capture File	**Notes**	Ctrl-Shift-O	Opens the Notes window that allows the user to add comments to a capture file.

Control Window **Live** Menu Selections

Mode	Selection	Hot-Key	Description
Live	**Start Capture**	Shift-F5	Begins data capture from the configured wireless devices.
	Stop Capture	F10	Stops data capture from the configured wireless devices.
	Clear	Shift-F10	Clears or saves the capture file.

Table 2.7 - Control Window **Options** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Hardware Settings**		0 - Classic 1 - *Bluetooth* low energy
	I/O Settings		0 - Classic 1 - *Bluetooth* low energy
	System Settings	Alt-Enter	Opens the System Settings dialog for configuring capture files.
	Directories...		Opens the File Locations dialog where the user can change the default file locations.
	Check for New Releases at Startup		When this selection is enabled, the program automatically checks for the latest Frontline protocol analyzer software releases.
	Side Names...		Opens the Side Names dialog used to customize the names of the slave and master wireless devices.
	Protocol Stack...		Opens the Select a Stack dialog where the user defines the protocol stack they want the analyzer to use when decoding frames.
	Set Initial Decoder Parameters...		Opens the Set Initial Decoder Parameters window. Each entry in the window takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. This selection is not present if no decoder is loaded that supports this feature.
	Set Subsequent Decoder Parameters...		Opens the Set Subsequent Decoder Parameters dialog where the user can override an existing parameter at any frame in the capture. Each entry takes effect from the specified frame onward or until redefined in this dialog on a later frame. This selection is not present if no decoder is loaded that supports this feature.
	Automatically Request Missing Decoder Information		When checked, this selection opens a dialog that asking for missing frame information. When unchecked, the analyzer decodes each frame until it cannot go further and it stops decoding. This selection is not present if no decoder is loaded that supports this feature.
	Enable/Disable Audio Expert System		When enabled, the Audio Expert System is active, other wise it is not available. Only available when an Audio Expert System licensed device is connected.

The **Windows** menu selection applies only to the **Control** window and open analysis windows: **Frame Display**, **Event Display**, **Message Sequence Chart**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**. All other windows, such as the datasource, are not affected by these selections.

Table 2.8 - Control Window **Windows** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Cascade**	Ctrl-W	Arranges open analysis windows in a cascaded view with window captions visible.
	Close All Views		Closes Open analysis windows.
	Minimize Control Minimizes All		When checked, minimizing the Control window also minimizes all open analysis windows.
	Frame Display and **Event Display**		When these windows are open the menu will display these selections. Clicking on the selection will bring that window to the front.

Control Window **Help** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Help Topics**		Opens the ComProbe Help window.
	About ComProbe Protocol Analysis System		Provides a pop-up showing the version and release information, Frontline contact information, and copyright information.
	Support on the Web		Opens a browser to fte.com technical support page.

2.3.6 Minimizing Windows

Windows can be minimized individually or as a group when the **Control** window is minimized. To minimize windows as a group:

1. Go to the **Window** menu on the **Control** window.
2. Select **Minimize Control Minimizes All**. The analyzer puts a check next to the menu item, indicating that when the **Control** window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

Chapter 3 Configuration Settings

In this section the ComProbe software is used to configure an analyzer for capturing data .

3.1 BPA 500 Configuration

3.1.1 BPA 500 - Update Firmware

When you select the Update Firmware on the BPA 500 Information, the Update ComProbe BPA 500 firmware dialog appears. You use this dialog to update your ComProbe hardware with the latest firmware.

It is very important that you update the firmware. If the firmware versions are not the same, you will not be able to start sniffing.

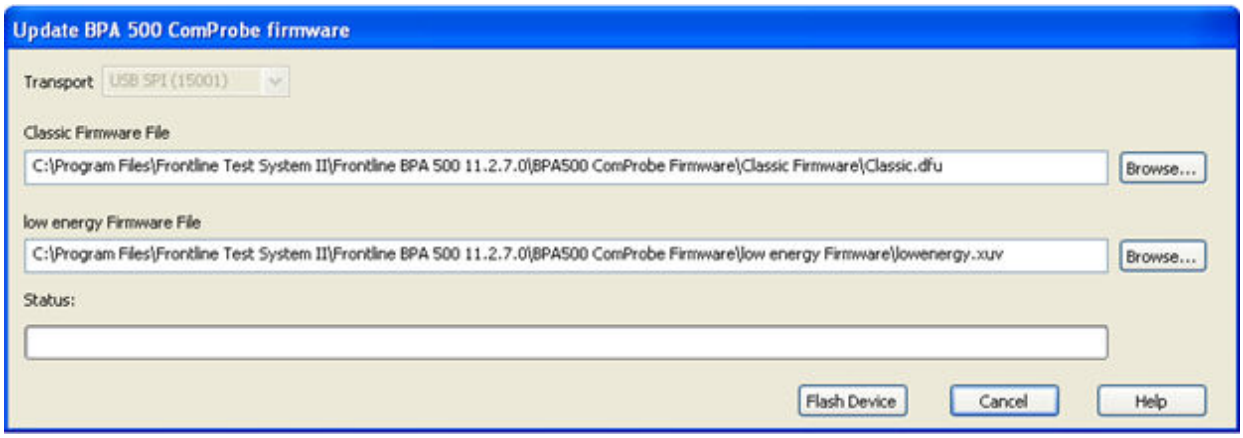


Figure 3.1 BPA 500 Update Firmware Dialog

1. Make sure the cabling is attached to the ComProbe hardware.

   Transport

Transport displays the ID number for the transport device(s) that you have connected. The device(s) will either be a USB to SPI converter or a SPI to LPT converter.

Classic Firmware File/low energy Firmware File

You do not have to change anything for the Classic Firmware File and low energy Firmware File.

2. Select Flash Device.

The download begins, with the Status bar displaying the progress. When the download is complete, you can check the firmware version by checking the Status dialog.

3.1.2 BPA 500 I/O Settings

3.1.2.1 Datasource Toolbar/Menu

The Datasource dialog toolbar and menu options are listed below.

Table 3.2 - BPA 500 Datasource Toolbar Icons

Icon	Descruption
	Start Sniffing button to begin sniffing. All settings are saved automatically when you start sniffing.
	Pause button to stop sniffing.
	When you select the Discover Devices button, the software lists all the discoverable *Bluetooth* devices on the Device Database dialog.
	Save button to save the configuration if you made changes but did not begin sniffing. All settings are saved automatically when you start sniffing.
	Help button opens the help file.

Table 3.3 - BPA 500 Datasource Menu

Menu Item	Description
File	Save and Exit options, self explanatory.
View	Hides or displays the toolbar.
BPA 500	Start Sniffing, Stop Sniffing, Resync Now, Discover Devices
Help	Opens ComProbe **Help**, and **About BPA 500**.

3.1.2.2 Selecting BPA 500 Devices Under Test

The Devices Under Test dialog has all the setup information the analyzer needs in order to synchronize with the piconet and capture data. The analyzer requires information on the clock synchronization method and the device address of the device to initially sync to. You must also choose what to sniff.

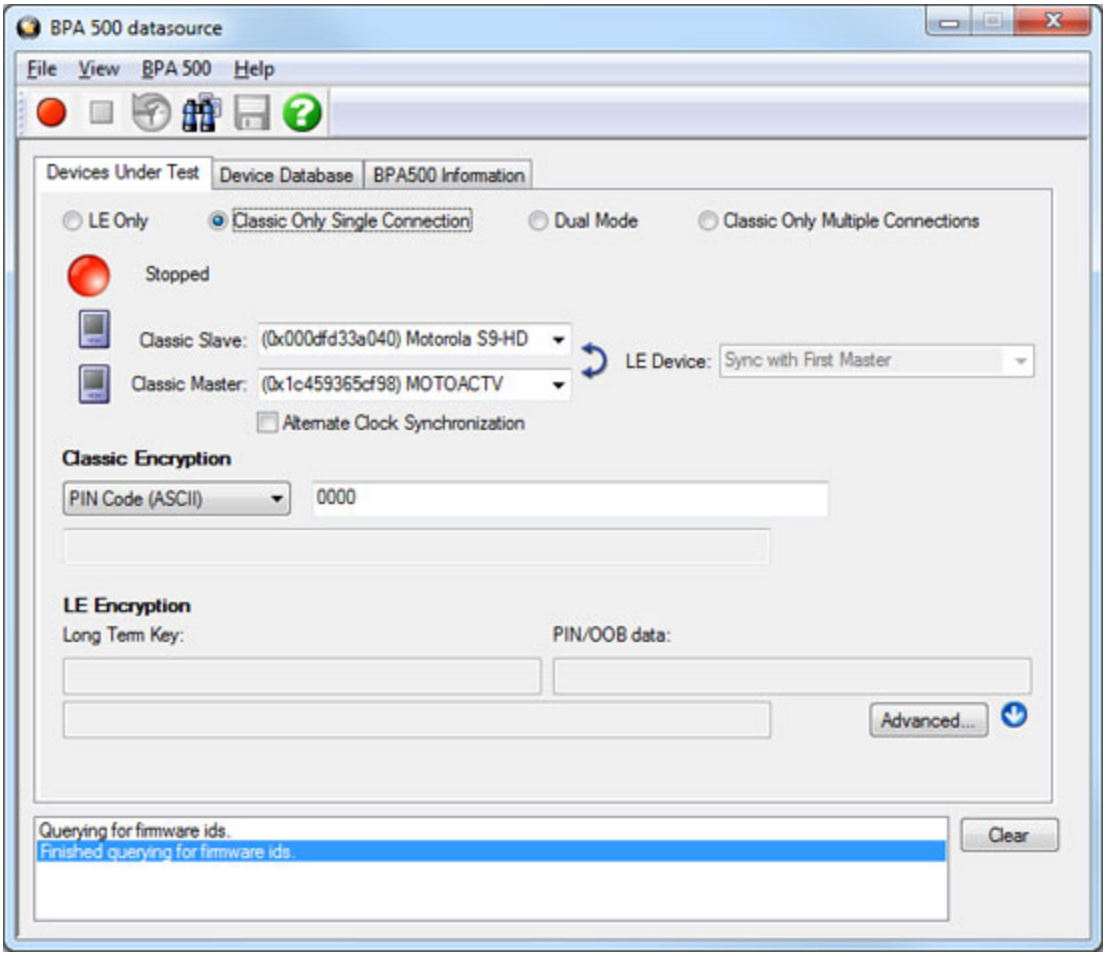


Figure 3.4 BPA 500 Datasource Dialog

You can choose to capture data using:

- low energy only
- Classic (BR/EDR) only
- Dual Mode - Combination of Classic and low energy
- Classic Only, Multiple Connections

Select one of these links above for explanations on how to configure each option.

There are a couple of other functions on the dialog that you need to understand.

Advanced

Click here to see the BPA 500 Advanced Classic Settings.

Channel Map

The Channel map shows which channels are available for Adaptive Frequency Hopping.

- **Channel Map** : Click this button to toggle on/off the display of the Channel Map.

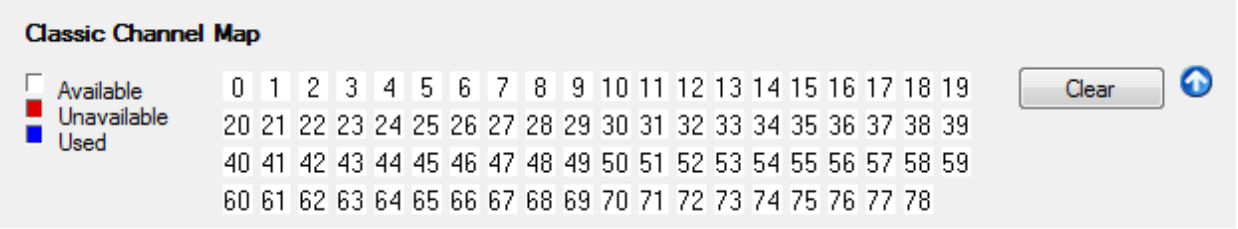


Figure 3.5 BPA 500 Classic Channel Map

This display is used to determine which channels are available with

Table 3.6 - Chanel Map Color Codes

Color	Indication
White	Channel is currently available for use.
Red	When Adaptive Frequency Hopping is in use, red indicates that the channel is marked as unavailable
Blue	Indicates that a packet was captured on the channel.

The **Clear** button resets each indicator back to the **White** state. The indicators are also reset whenever a new **Channel Map** goes into effect.

Status Window

A status window at the bottom of the dialog displays information about recent activity.

3.1.2.3 BPA 500 Devices Under Test

3.1.2.3.1 BPA 500 - Devices Under Test - LE Only

There are four ways to sniff Bluetooth® wireless technology communications using the ComProbe BPA 500 Dual Mode *Bluetooth* Protocol Analyzer. You choose the mode you will be using by selecting one of the following radio buttons on the Devices Under Test tab in the BPA 500 datasource dialog:

1. LE Only
2. Classic Only Single Connection
3. Dual Mode
4. Classic Only Multiple Connections

Setup - LE Only

By selecting the "LE Only" radio button under the "Devices Under Test" tab you can configure the BPA 500 protocol analyzer for sniffing Bluetooth low energy communications.

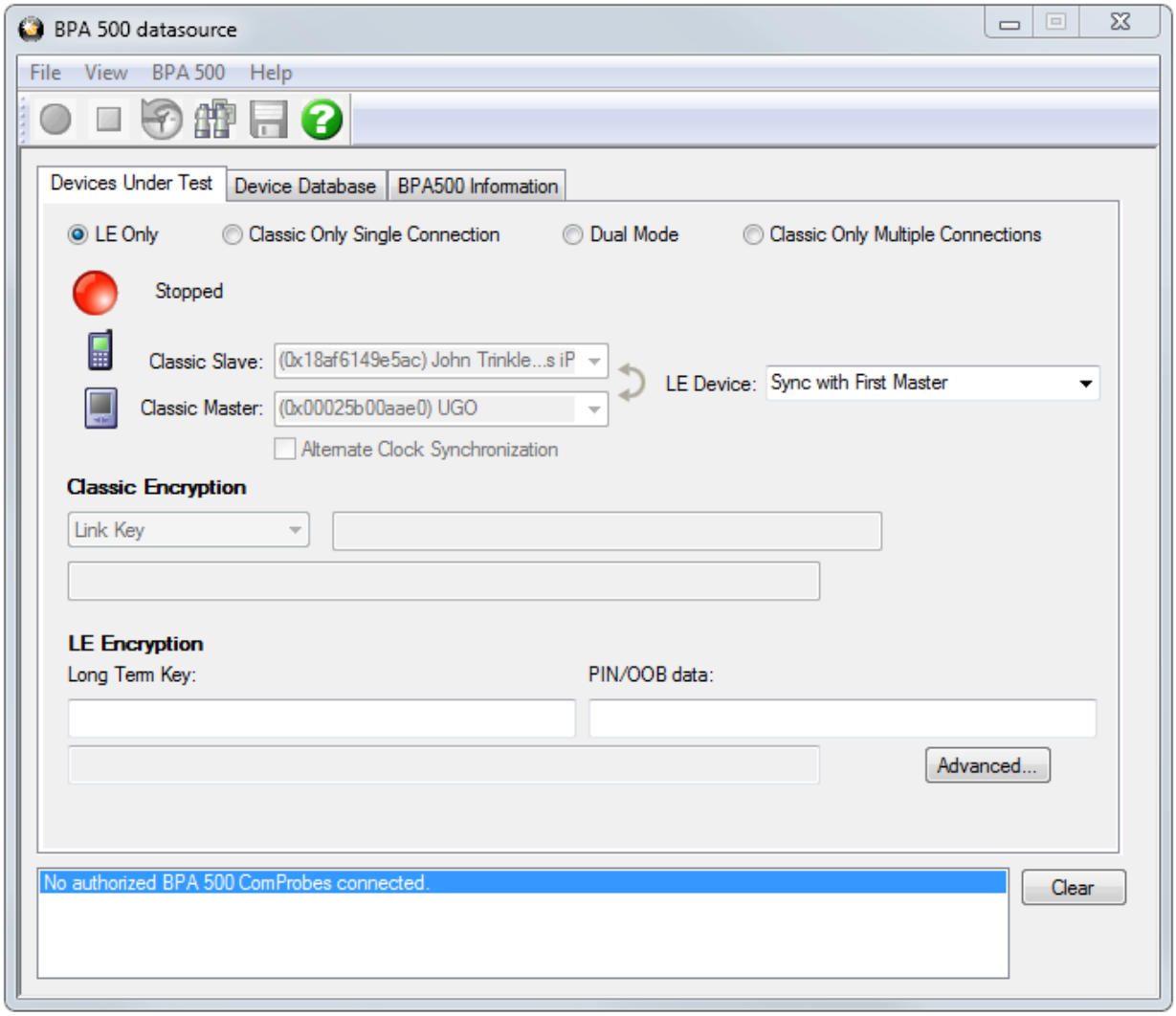


Figure 3.7 BPA 500 Devices Under Test - LE Only Tab

The default value in the "LE Device" drop down is "Sync with First Master". To begin sniffing *Bluetooth* low energy simply click the red button to start. The analyzer will capture packets from the first Master that makes a connection . To capture the advertising traffic and the connection(s), you must specify a device address.

Specifying the LE Device Address

1. If you would like you may specify the LE device you are testing by typing in or choosing its address (BD_ ADDR). You can type it directly into the drop down, or choose it from the existing previous values list in the drop down.

To enter the device manually type the address - 12 digit hex number (6 octets). The "0x" is automatically typed in the drop down control.

Once you have the devices address identified, the next step is to identify the Encryption.

LE Encryption

Figure 3.8 BPA 500 LE Encryption

2. Enter the Long Term Key for the Encryption.

The Long Term Key is similar to the Link key in Classic. It is a persistent key that is stored in both devices and used to derive a fresh encryption key each time the devices go encrypted.

There are a few differences though:

In Classic the Link key is derived from inputs from both devices and is calculated in the same way independently by both devices and then stored persistently. The link key itself is never transmitted over the air during pairing

In LE, the long term key is generated solely on the slave device and then, during pairing, is distributed to a master device that wants to establish an encrypted connection to that slave in the future. Thus the long term key is transmitted over the air, albeit encrypted with a one-time key derived during the pairing process and discarded afterwards (the so called short term key).

Unlike the link key, this long term key is directional, i.e. it is only used to for connections from the master to the slave (referring to the roles of the devices during the pairing process). If the devices also want to connect the other way round in the future, the device in the master role (during the pairing process) also needs to send its own long term key to the device in the slave role during the pairing process (also encrypted with the short term key of course), so that the device which was in the slave during the pairing process can be a master in the future and connect to the device which was master during the pairing process (but then would be in a slave role).

Since most simple LE devices are only ever slave and never master at all, the second long term key exchange is optional during the pairing process.

Note: If you use Copy/Paste to insert the Long Term Key , Frontline will auto correct (remove invalid white spaces) to correctly format the key.

3. Enter a PIN or out-of-band (OOB) value for Pairing.

This optional information offers alternative pairing methods.

One of two pieces of data allow alternative pairing:

1. PIN is a six-digit (or less if leading zeros are omitted) decimal number.
2. Out-of-Band (OOB) data is a 16-digit hexadecimal code which the devices exchange via a channel that is different than the le transmission itself. This channel is called OOB

   For off-the-shelf devices we cannot sniff OOB data, but in the lab you may have access to the data exchanged through this channel.

Click here to see how to capture data after completing the configuration.

3.1.2.3.2 BPA 500 - Devices Under Test - Classic Only Single Connection

There are four ways to sniff Bluetooth® wireless technology communications using the ComProbe BPA 500 Dual Mode *Bluetooth* Protocol Analyzer. You choose the mode you will be using by selecting one of the following radio buttons on the Devices Under Test tab in the BPA 500 datasource dialog:

1. LE Only
2. Classic Only Single Connection
3. Dual Mode
4. Classic Only Multiple Connections

Setup - Classic Only Single Connection

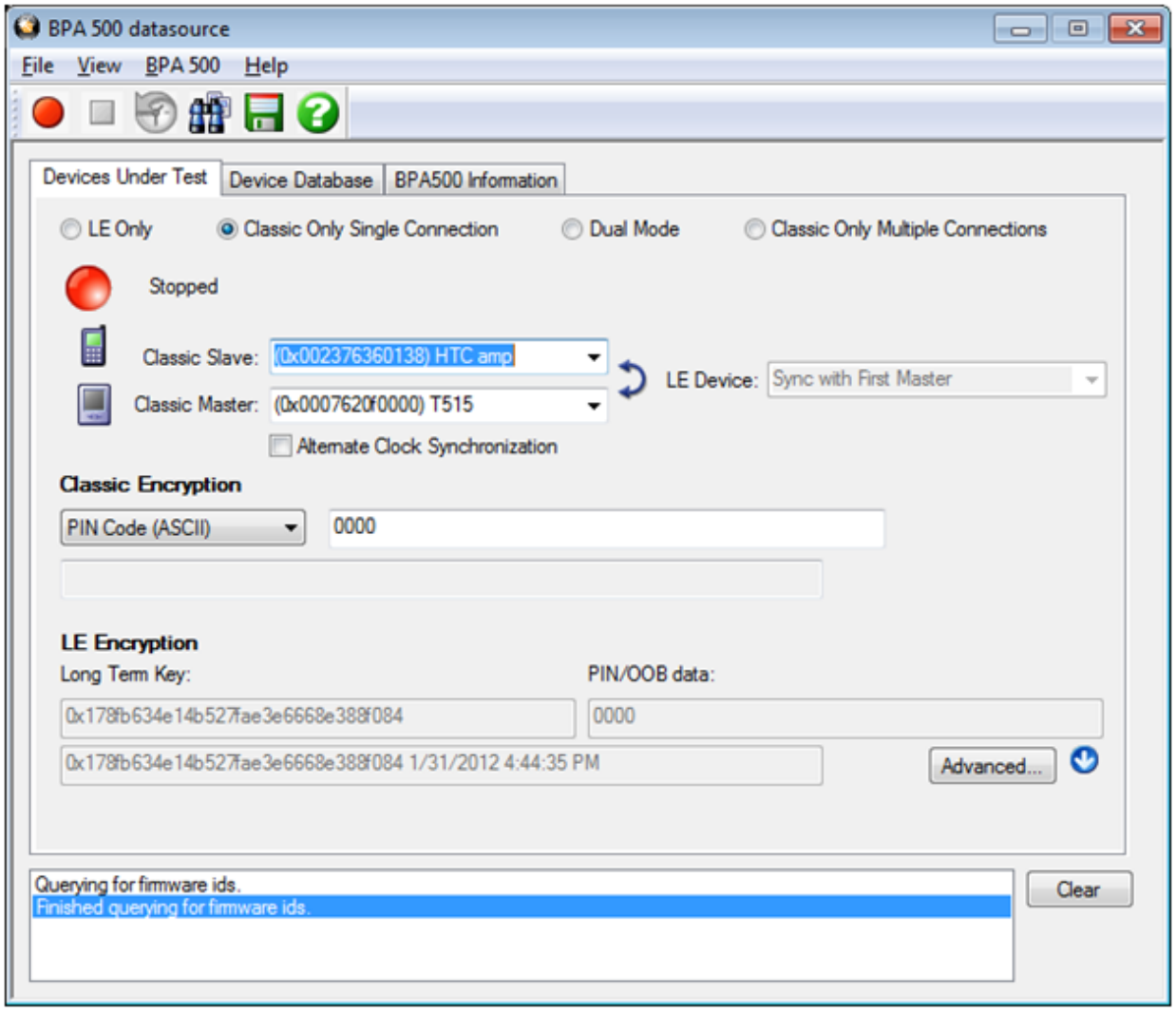
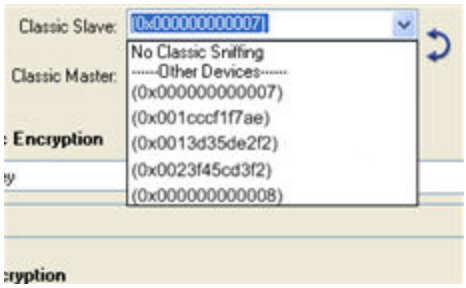


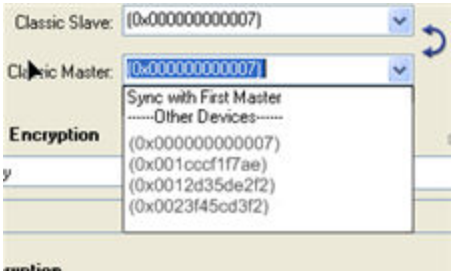
Figure 3.9 BPA 500 Devices Under Test - Classic Only Single Connection

Specifying the Bluetooth Device Address (BD_ADDR)

The analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for the Slave and the Master. You can specify the *Bluetooth* Device Address in multiple ways.



1. Select the *Bluetooth* Device Address (BD_ADDR) for Classic Slave: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.
2. Select the *Bluetooth* Device Address (BD_ADDR) for Classic Master: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



Classic Encryption

Once you have the devices address identified, the next step is to identify the Encryption.

Figure 3.10 BPA 500 Classic Encrytion

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.

There are three encryption options in the I/O Settings dialog.

1. PIN Code (ASCII)
2. PIN Code (Hex)
3. Link Key

You are able to switch between these methods in the I/O Settings window. When you select a method, a note appears at the bottom of the dialog reminding you what you need to do to successfully complete the dialog.

- The first and second options use a PIN Code to generate the Link Key. The devices generate link Keys during the Pairing Process based on a PIN Code. The Link Key generated from this process is also based on a random

number so the security cannot be compromised. If the analyzer is given the PIN Code it can determine the Link Key using the same algorithm. Since the analyzer also needs the random number, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

Example:

If the ASCII character PIN Code is **ABC** and you choose to enter the ASCII characters, then select **PIN Code (ASCII)** from the Encryption drop down list and enter **ABC** in the field below.

If you choose to enter the Hex equivalent of the ASCII character PIN Code **ABC**, then select **PIN Code (Hex)** from the Encryption drop down list and enter **0x414243** in the field. Where **41** is the Hex equivalent of the letter **A**, **42** is the Hex equivalent of the letter **B**, and **43** is the Hex equivalent of the letter **C**.

Note: When **PIN Code (Hex)** is selected from the Encryption drop down list, the **0x** prefix is entered automatically.

- Third, if you know the Link Key in advance you may enter it directly. Select Link Key in the Encryption list and then enter the Link Key in the edit box. If the link key is already in the database, the Link Key is automatically entered in the edit box after the Master and Slave have been selected. You can also pick **Choose Pair from Device Database** to select a Master, Slave and Link Key from the Device Database.

  When the devices are in the debug mode Secure Simple Pairing (SSP) is automatically supported with no configuration. We support SSP when the devices are not in the debug mode if they have the private key of one of the devices. Contact Frontline technical support for further assistance with this process.

  - Select an Encryption option.
  - Enter a value for the encryption.

3.1.2.3.3 BPA 500 - Devices Under Test - Dual Mode

There are four ways to sniff Bluetooth® wireless technology communications using the ComProbe BPA 500 Dual Mode Bluetooth Protocol Analyzer. You choose the mode you will be using by selecting one of the following radio buttons on the Devices Under Test tab in the BPA 500 datasource dialog:

1. LE Only
2. Classic Only Single Connection
3. Dual Mode
4. Classic Only Multiple Connections

Note: When selecting and using either "Dual Mode" or "Classic Only Multiple Connection" you must connect both antennas (LE and Classic) to the ComProbe BPA 500 hardware.

Setup - Dual Mode

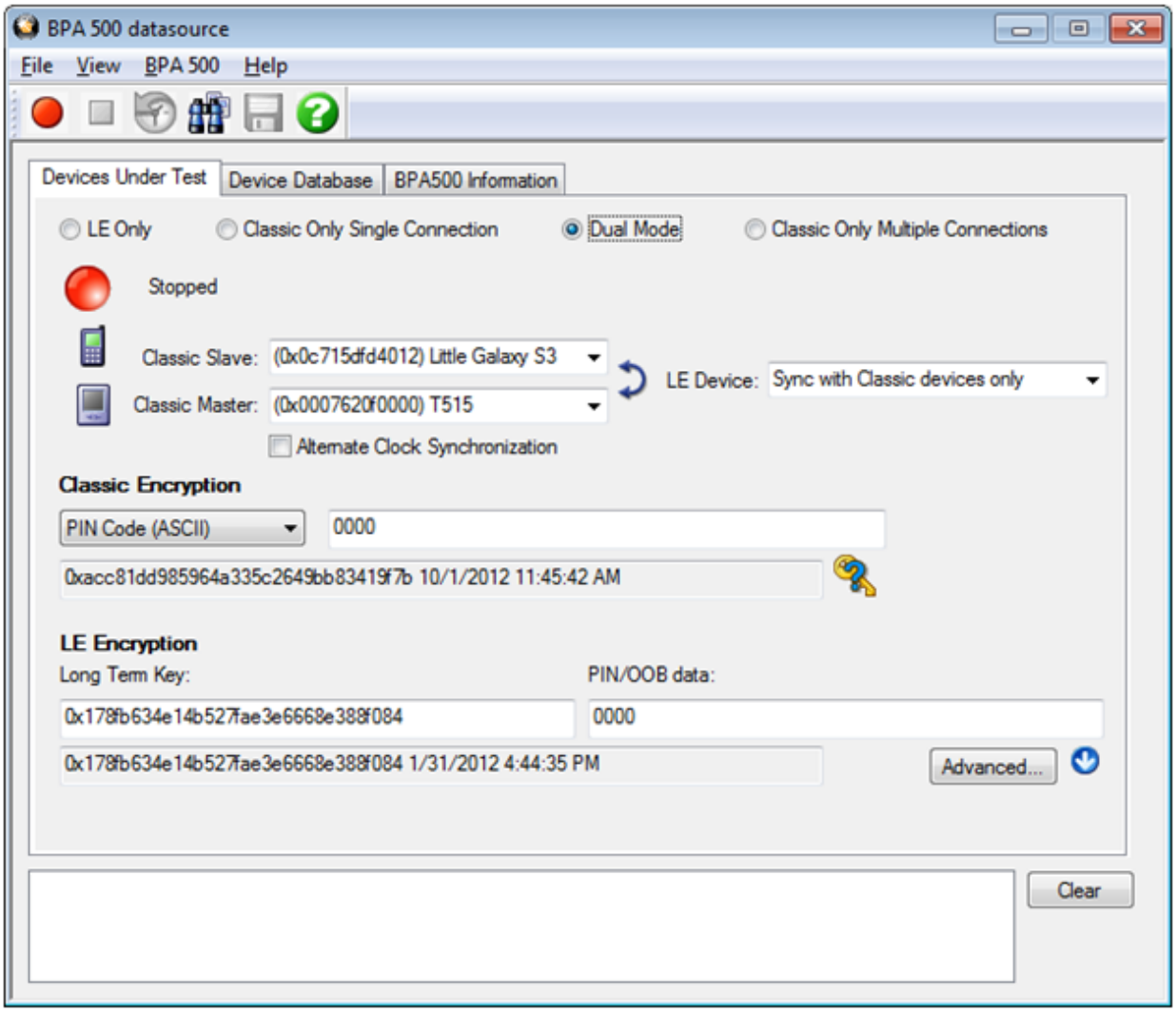
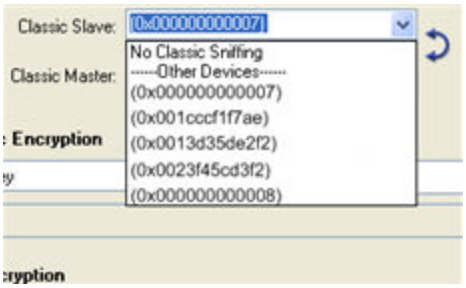


Figure 3.11 BPA 500 Devices under Test - Dual Mode

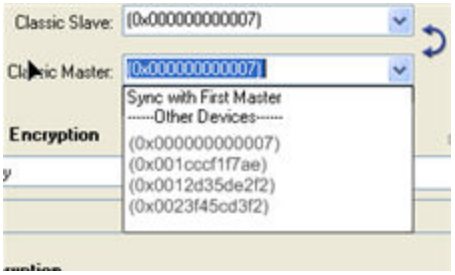
Specifying the *Bluetooth* Device Address (BD_ADDR)

The analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for the Slave and the Master. You can specify the *Bluetooth* Device Address in multiple ways.

1. Select the *Bluetooth* Device Address (BD_ADDR) for Classic Slave: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



2. Select the *Bluetooth* Device Address (BD_ADDR) for **Classic Master**: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



3. Specify the BD_ADDR for the LE Device by selecting "Sync with Classic Devices Only". By doing this, the low energy device will follow connections from or to the specified device, or from or to the first Classic device that connects over LE.

Classic Encryption

Figure 3.12 BPA 500 Classic Encryption

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.

There are three encryption options in the I/O Settings dialog.

a. PIN Code (ASCII)

b. PIN Code (Hex)

c. Link Key

- The firs tand second options use a PIN Code to generate the Link Key. The devices generate link Keys during the pairing process based on a PIN Code. The second Link Key generated from this process is also based on a random number so the security cannot be compromised. If the analyzer is given the PIN Code it can

determine the Link Key using the same algorithm. Since the analyzer also needs the random number, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

Example:

If the ASCII character PIN Code is ABC and you choose to enter the ASCII characters, then select PIN Code (ASCII) from the Encryption drop down list and enter ABC in the field below.

If you choose to enter the Hex equivalent of the ASCII character PIN Code ABC, then select PIN Code (Hex) from the Encryption drop down list and enter 0x414243 in the field. Where 41 is the Hex equivalent of the letter A, 42 is the Hex equivalent of the letter B, and 43 is the Hex equivalent of the letter C.

Note: When PIN Code (Hex) is selected from the Encryption drop down list, the 0x prefix is entered automatically.

- Third, if you know the Link Key in advance you may enter it directly. Select Link Key in the Encryption list and then enter the Link Key in the edit box. If the link key is already in the database, the Link Key is automatically entered in the edit box after the Master and Slave have been selected. You can also pick Choose Pair from Device Database to select a Master, Slave and Link Key from the Device Database.

1. Select an Encryption option.
2. Enter a value for the encryption.

LE Encryption

BPA 500 LE Encryption

1. Enter the **Long Term Key** for the **LE Encryption**.

   The **Long Term Key** is similar to the Link key in Classic. It is a persistent key that is stored in both devices and used to derive a fresh encryption key each time the devices go encrypted.

   There are a few differences though:

   In Classic the Link key is derived from inputs from both devices and is calculated in the same way independently by both devices and then stored persistently. The link key itself is never transmitted over the air during pairing.

   In LE, the long term key is generated solely on the slave device and then, during pairing, is distributed to a master device that wants to establish an encrypted connection to that slave in the future. Thus the long term key is transmitted over the air, albeit encrypted with a one-time key derived during the pairing process and discarded afterwards (the so called short term key).

   Unlike the link key, this long term key is directional, i.e. it is only used to for connections from the master to the slave (referring to the roles of the devices during the pairing process). If the devices also want to connect the other way round in the future, the device in the master role (during the pairing process) also needs to send its own long term key to the device in the slave role during the pairing process (also encrypted with the short term key of course), so that the device which was in the slave during the pairing process can be a master in the future and connect to the device which was master during the pairing process (but then would be in a slave role).

Since most simple LE devices are only ever slave and never master at all, the second long term key exchange is optional during the pairing process.

Note: If you use Copy/Paste to insert the Long Term Key , Frontline will auto correct (remove invalid white spaces) to correctly format the key.

2. Enter a PIN or out-of-band (OOB) value for Pairing.

This optional information offers alternative pairing methods.

One of two pieces of data allow alternative pairing:

1. PIN is a six-digit (or less if leading zeros are omitted) decimal number.
2. Out-of-Band (OOB) data is a 16-digit hexadecimal code which the devices exchange via a channel that is different than the le transmission itself. This channel is called OOB.

   For off-the-shelf devices we cannot sniff OOB data, but in the lab you may have access to the data exchanged through this channel.

3.1.2.3.4 BPA 500 - Devices Under Test - Classic Only Multiple Connection

There are four ways to sniff Bluetooth® wireless technology communications using the ComProbe BPA 500 Dual Mode *Bluetooth* Protocol Analyzer. You choose the mode you will be using by selecting one of the following radio buttons on the Devices Under Test tab in the BPA 500 datasource dialog:

1. LE Only
2. Classic Only Single Connection
3. Dual Mode
4. Classic Only Multiple Connections

Note: When selecting and using either "Dual Mode" or "Classic Only Multiple Connection" you must connect both antennas (LE and Classic) to the ComProbe BPA 500 hardware.

Setup - Classic Only Multiple Connections

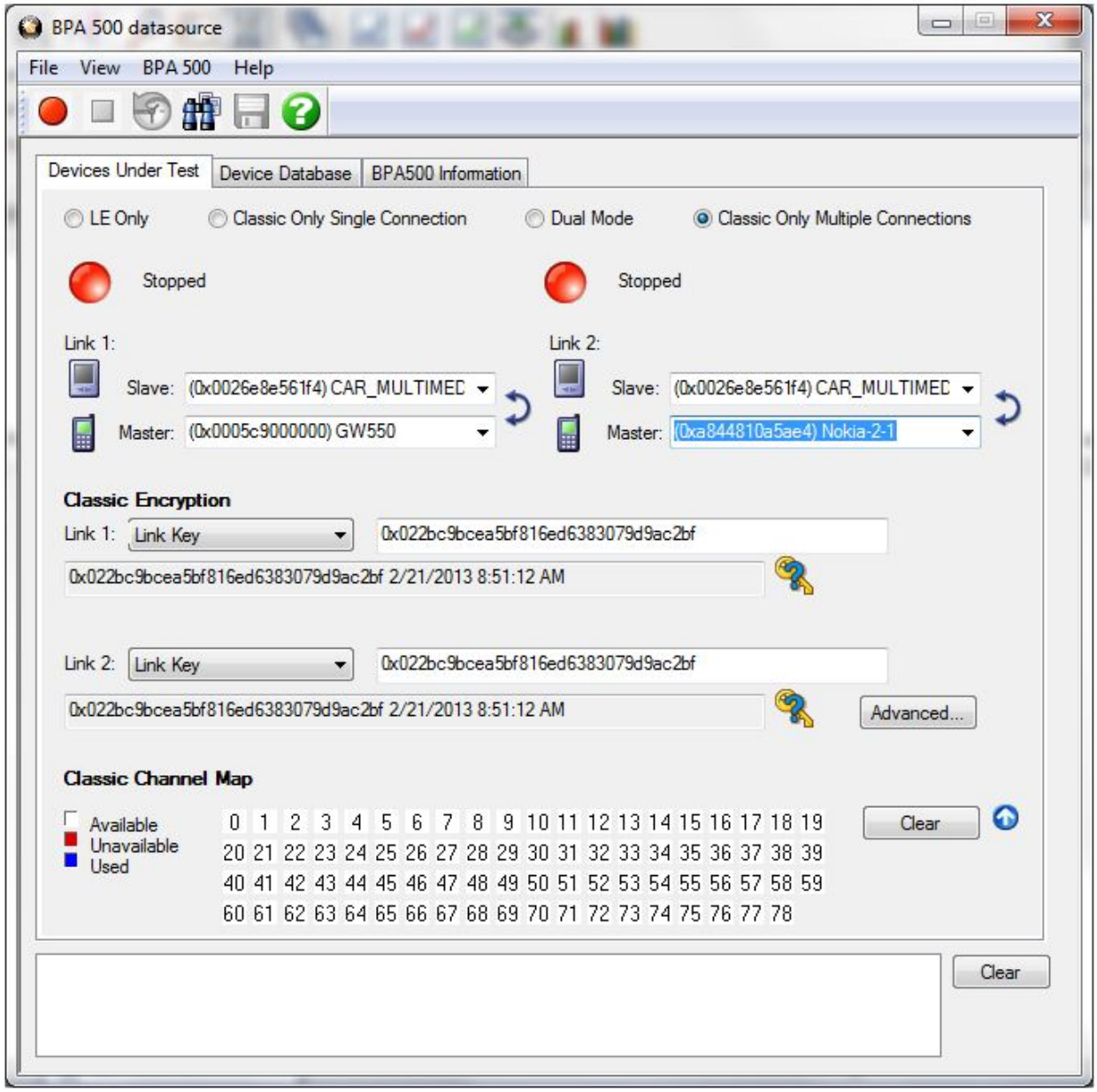
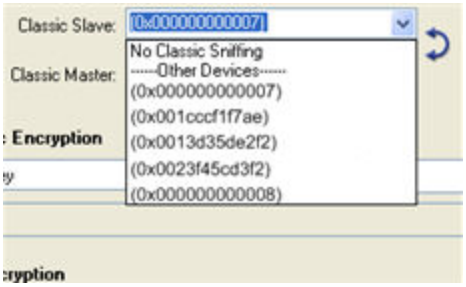

BPA 500 datasource
File View BPA 500 Help
Devices Under Test
Device Database
BPA500 Information
LE Only
Classic Only Single Connection
Dual Mode
Classic Only Multiple Connections
Stopped
Stopped
Link 1:
Slave: (0x0026e8e561f4) CAR_MULTIMED
Master: (0x0005c9000000) GW550
Link 2:
Slave: (0x0026e8e561f4) CAR_MULTIMED
Master: (0xa844810a5ae4) Nokia-2-1
Classic Encryption
Link 1: Link Key
0x022bc9bcea5bf816ed6383079d9ac2bf
0x022bc9bcea5bf816ed6383079d9ac2bf 2/21/2013 8:51:12 AM
Link 2: Link Key
0x022bc9bcea5bf816ed6383079d9ac2bf
0x022bc9bcea5bf816ed6383079d9ac2bf 2/21/2013 8:51:12 AM
Advanced...
Classic Channel Map
Available
Unavailable
Used
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78
Clear
Clear

Figure 3.13 BPA 500 Devices Under Test - Classic Only Multiple Connections

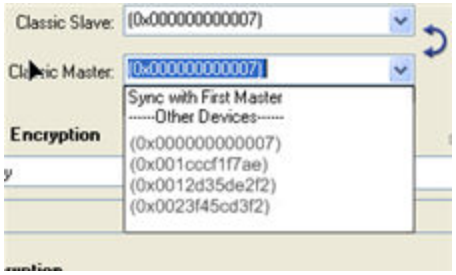
Specifying the *Bluetooth* Device Address (BD_ADDR)

The analyzer needs to know the *Bluetooth* Device Address (BD_ADDR) for the Slave and the Master. You can specify the *Bluetooth* Device Address in multiple ways.

1. Select the *Bluetooth* Device Address (BD_ADDR) for Classic Slave: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



2. Select the *Bluetooth* Device Address (BD_ADDR) for Classic Master: from a list of available devices from the Device Database. You can also type in the address as a 12 digit hex number (6 octets). The "0x" is automatically typed in by the control. Any devices entered this way is added to the Device Database.



Classic Encryption

Figure 3.14 BPA 500 Classic Encryption

Bluetooth devices can have their data encrypted when they communicate. *Bluetooth* devices on an encrypted link share a common link key in order to exchange encrypted data. How that link key is created depends upon the pairing method used.

There are three encryption options in the I/O Settings dialog.

- PIN Code (ASCII)
- PIN Code (Hex)
- Link Key

You are able to switch between these methods in the I/O Settings window. When you select a method, a note appears at the bottom of the dialog reminding you what you need to do to successfully complete the dialog.

- The first and second options use a PIN Code to generate the Link Key. The devices generate link Keys during the Pairing Process based on a PIN Code. The Link Key generated from this process is also based on a random number so the security cannot be compromised. If the analyzer is given the PIN Code it can determine the Link Key using the same algorithm. Since the analyzer also needs the random number, the analyzer must catch the entire Pairing Process or else it cannot generate the Link Key and decode the data.

  Example:

If the ASCII character PIN Code is ABC and you choose to enter the ASCII characters, then select PIN Code (ASCII) from the Encryption drop down list and enter ABC in the field below.

If you choose to enter the Hex equivalent of the ASCII character PIN Code ABC, then select PIN Code (Hex) from the Encryption drop down list and enter 0x414243 in the field. Where 41 is the Hex equivalent of the letter A, 42 is the Hex equivalent of the letter B, and 43 is the Hex equivalent of the letter C.

Note: When PIN Code (Hex) is selected from the Encryption drop down list, the 0x prefix is entered automatically.

- Third, if you know the Link Key in advance you may enter it directly. Select Link Key in the Encryption list and then enter the Link Key in the edit box. If the link key is already in the database, the Link Key is automatically entered in the edit box after the Master and Slave have been selected. You can also pick Choose Pair from Device Database to select a Master, Slave and Link Key from the Device Database.

When the devices are in the debug mode Secure Simple Pairing (SSP) is automatically supported with no configuration. We support SSP when the devices are not in the debug mode if they have the private key of one of the devices. Contact Frontline technical support for further assistance with this process.

1. Select an Encryption option.
2. Enter a value for the encryption.

3.1.2.3.5 Programmatically Update Link Key from 3rd Party Software

Now the BPA 600 protocol analyzer user can update the link keys for either of the classic links using a very common Windows message WM_COPYDATA. The mechanism is to send a WM_COPYDATA message to the BPA 600 datasource.

The best scenario for doing this is when the devices are doing SSP and they are NOT in debug mode. The following is a snippet of code that gives an example of programmatically sending link key to the ComProbe Protocol Analysis System software. In order to do this the user needs to know both addresses of the devices in the link for which they wish to update the link key. Also, the Datasource expects the master and slave addresses in LSB to MSB format.

If the link key is sent to ComProbe software after encryption has been turned on over the air, ComProbe software will flag an error on the Start Encryption packet. Depending on when the link key has been sent down, ComProbe software may however still be able to sniff the link successfully. In order to guarantee that ComProbe software is able to sniff the link the link key should be sent to ComProbe software as soon as it is available and before encryption has been turned on over the air.

Use the following code for BPA 600:

```
#define HCI_LINK_KEY 1000

    HWND nHandle = ::FindWindow(NULL,"BPA 600 datasource");
    if(nHandle != 0)
    {

        COPYDATASTRUCT ds;
        enum
        {
```

```
        EncryptionKeySize = 16,
        sizeAddressDevice = 6

    };
    BYTE abytAddressDevice1[sizeAddressDevice] = { 0x12, 0x34, 0x56, 0x78, 0x9a, 0xbc }; //LSB-
        >MSB
    BYTE abytAddressDevice2[sizeAddressDevice] = { 0x21, 0x43, 0x65, 0x87, 0xa9, 0xcb };
    BYTE abytLinkKey[EncryptionKeySize] = { 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff,
        0xff, 0xff, 0xff, 0xff, 0xff, 0xff };
    ds.cbData = sizeAddressDevice + sizeAddressDevice + EncryptionKeySize;
    ds.dwData = HCI_LINK_KEY;
    BYTE bytData[sizeAddressDevice + sizeAddressDevice + EncryptionKeySize];
    memcpy(&bytData,&abytAddressDevice1,sizeAddressDevice);
    memcpy(&bytData[sizeAddressDevice],&abytAddressDevice2,sizeAddressDevice);
    memcpy(&bytData
        [sizeAddressDevice+sizeAddressDevice],&abytLinkKey,EncryptionKeySize);
    ds.lpData = &bytData;
    ::SendMessage(nHandle, WM_COPYDATA, (WPARAM)GetSafeHwnd(), (LPARAM)&ds);

}
```

3.1.2.4 BPA 500 Device Database

The Device Database contains information about the devices that have been discovered or entered by the user when using BPA 500 protocol analyzer.

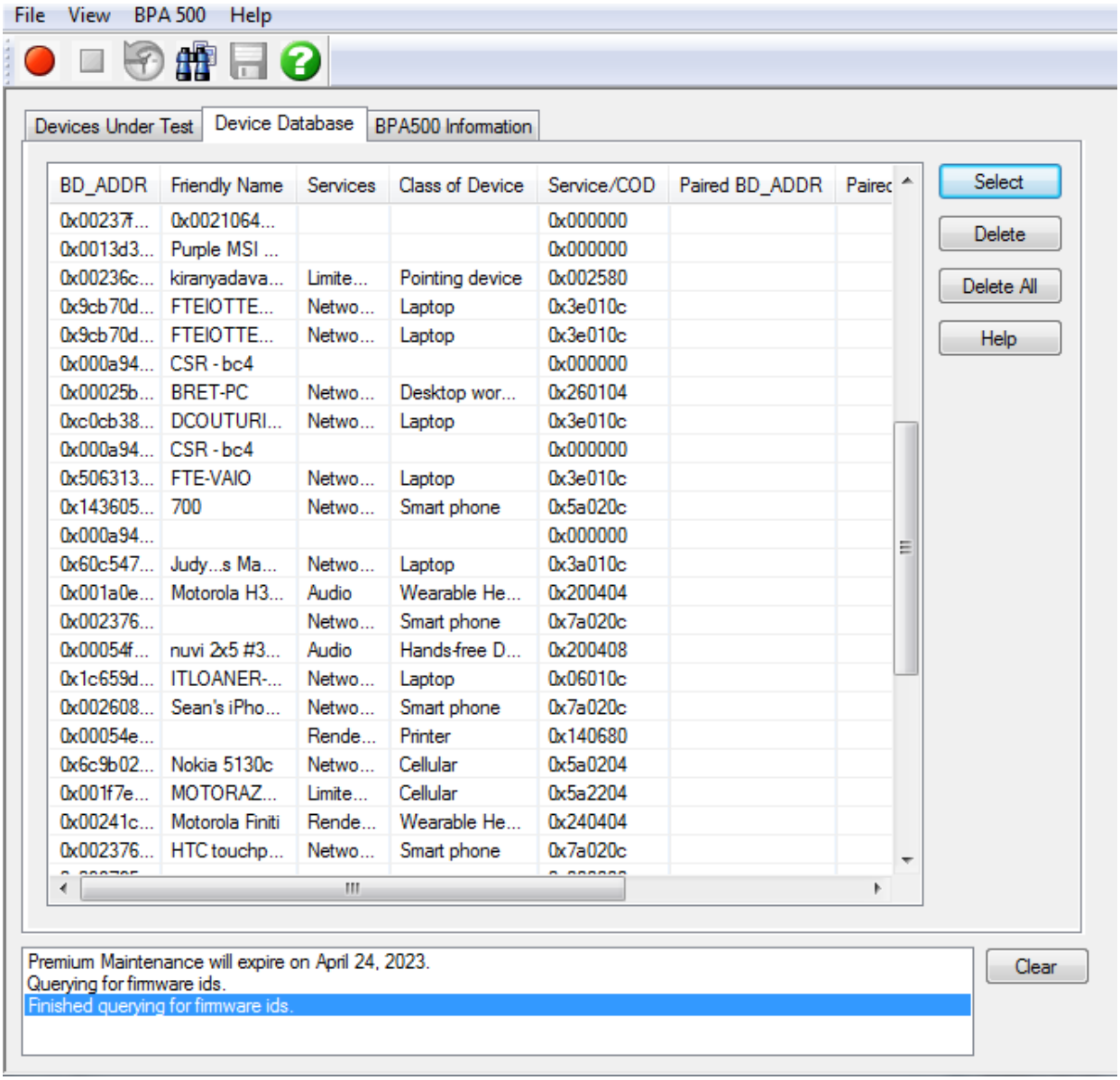


Figure 3.15 BPA 500 Datasource Device Database Tab

The Device Database is automatically updated when you perform certain operation like initiating a Refresh Device List or entering encryption information from the Devices Under Test dialog.

- When you select the Discover button, BPA 500 software lists all the discoverable *Bluetooth* devices.
- When you select a device from the list, then click Select, the information is transferred to the Devices Under Test dialog.
- You can delete records one at a time by selecting the record, then selecting **Delete**.
- You can also delete all the records by selecting Delete All.

- Select Close to close the dialog.
- The Help button brings up more Help information.
- A message box at the bottom of the dialog displays the BPA 500 devices that are connected.

3.1.2.5 BPA 500 Information

The BPA 500 Information dialog is one of the three tabs that appear when you first start BPA 500 protocol analyzer software.

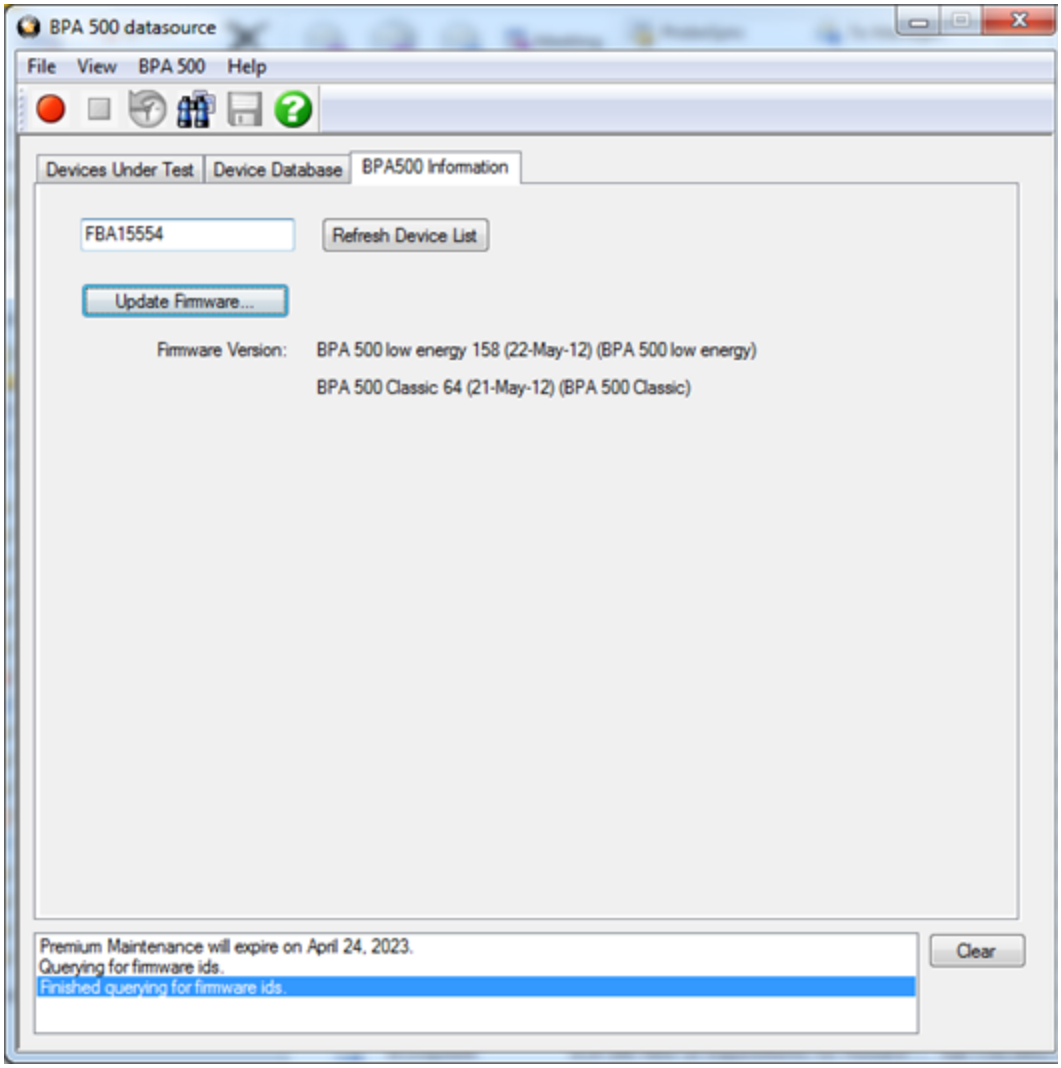


Figure 3.16 BPA 500 Datasource Information Tab

Note: You can also access these three by selecting I/O Settings or Hardware Settings from the Options menu on the Control Window toolbar.

There are several pieces of information on this display:

- The current firmware is displayed under Firmware Version.
- If you want to make sure the most up-to-date list of devices is shown, select Refresh Device list.
- If you want to load the latest firmware, you select the Update Firmware button.
- A message box at the bottom of the dialog displays the BPA 500 devices that are connected.

3.1.2.6 BPA 500 Advanced Classic Settings

The Advanced Classic Settings dialog contains additional options for synchronizing the analyzer with the link to capture data.

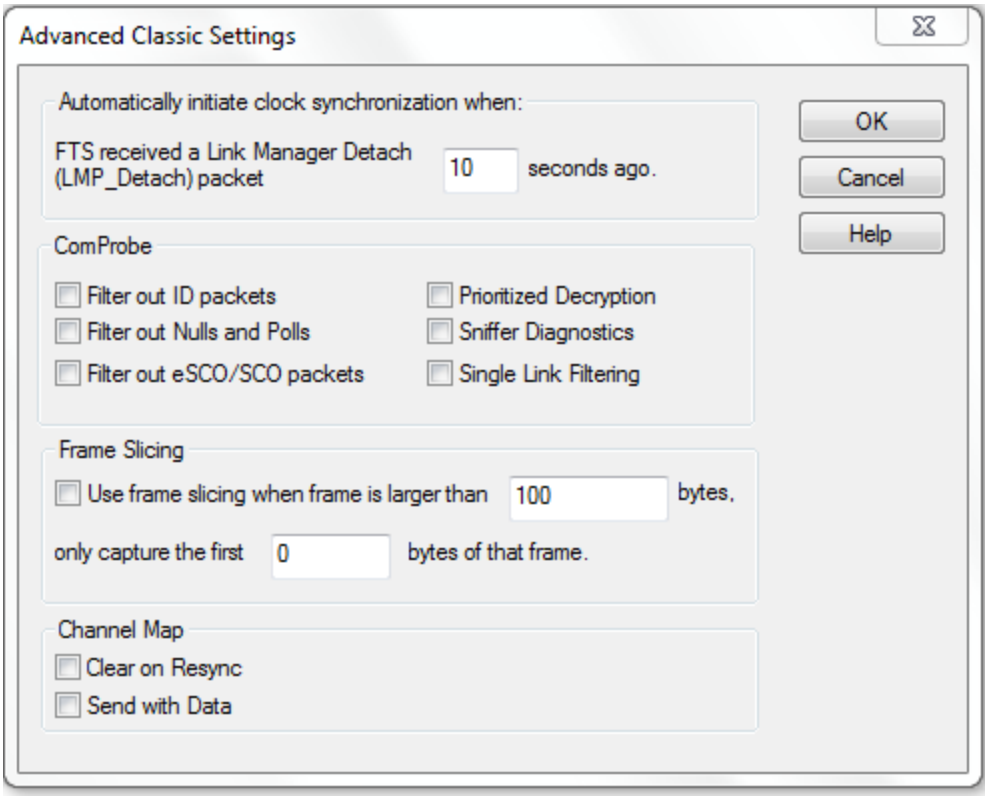


Figure 3.17 BPA 500 Datasource Devices Under Test Advance Classic Settings Dialog

1. Automatically initiate Clock Synchronization Options

   - If you would like to have the analyzer re-synchronize when a Link Manager Detach (LMP_Detach) packet is received after a specific period of time or when the ComProbe® analyzer has not been locked to the Master Clock, you must select the option here and set the time period.

     This option is not automatically available if either **Classic Only Single Connection**, **Dual Mode**, or **Classic Only Multiple Connections** was selected in the Devices Under Test tab. To activate this option you must have checked **Alternate Clock Synchronization** in the **Devices Under Test** tab. If the box was not checked the **seconds ago** box is grayed out. For low energy devices this option is automatically selected.

2. **ComProbe**

   Some packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display window. You have several options to exclude certain types of packets.

   - **Filter out ID packets** - When this is checked, all ID packets are filtered out.
   - **Filter out Nulls and Polls** - When this is checked, Nulls and Polls packets are filtered out.
   - **Filter out SCO/eSCO** - When this is checked, SCO/eSCO packets are filtered out.
   - **Prioritized Decryption** can be selected if you are having trouble establishing the correct decryption. This option adjusts the data capture to give priority to establishing the proper decryption over receiving frames. If you select this option, some frames may be dropped, but establishing the decryption key will be more efficient.
   - **Sniffer Diagnostics** - When this is checked, some diagnostic data from the ComProbe are captured and stored in the .cfa file. This is useful when a .cfa file is sent to Frontline for analysis and diagnosis. Technical Support may ask you to check this option when you are experiencing issues with BPA 500.
   - **Single Link Filtering** - When this is checked, only packets from the specific Master and Slave selected in Devices Under Test are displayed. Data from other devices that may be connected to the Master will be filtered out.

3. **Frame Slicing Settings**

   - Frame Slicing Settings allows you to enter the size of the largest frame allowed to pass the analyzer without having any bytes removed. The second field tells the analyzer the number of bytes you would like to capture if the frame is larger than the allowable value indicated in the first field.

4. **Channel Map**

   - Clear on Resync -used to clear the map each time a re-synchronization occurs
   - Send with Data - allows you to send a map each time data is sent instead of just sending a map when changes occur.

3.2 Decoder Parameters

Some protocol decoders have user-defined parameters. These are protocols where some information cannot be discovered by looking at the data and must be entered by the user in order for the decoder to correctly decode the data. For example, such information might be a field where the length is either 3 or 4 bytes, and which length is being used is a system option.

There may be times when the context for decoding a frame is missing. For example, if the analyzer captures a response frame but does not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** window allows you to supply the context for any frame. The dialog allows you to define any number of parameters and save them in a template for later use

The decoder template function provides the capacity to create multiple templates that contain different parameters. This capability allows you to maintain individual templates for each Bluetooth® network monitored. Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

If you have decoders loaded which require decoder parameters, a window with one tab for every decoder that requires parameters appears the first time the decoder is loaded.

For help on setting the parameters, click the **Help** button on each tab to get help information specific to that decoder.

If you need to change the parameters later,

- Choose **Set Initial Decoder Parameters...** from the **Options** menu on the **Control** and **Frame Display** windows.

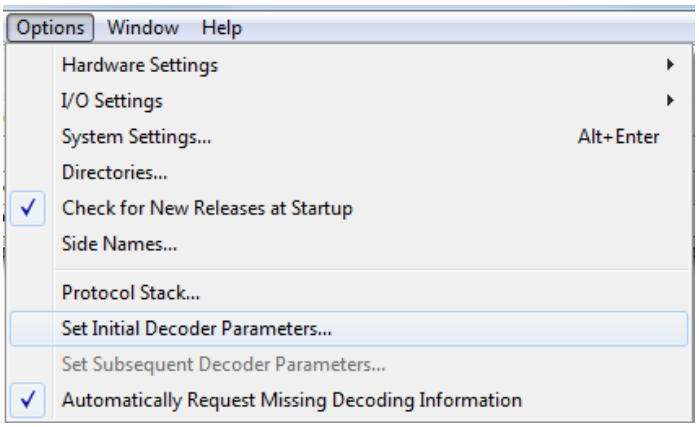


Figure 3.1 - Select **Set Initial Decoder Parameters...** from **Control** window

The **Set Initial Decoder Parameters** window opens with a tab for each decoder that requires parameters.

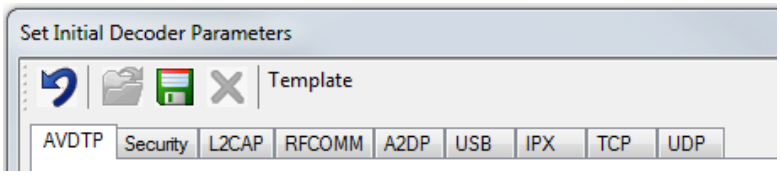


Figure 3.2 - Tabs for each decoder requiring parameters.

- Each entry in the **Set Initial Decoder Parameters** window takes effect from the beginning of the capture onward or until redefined in the **Set Subsequent Decoder Parameters** dialog.

Override Existing Parameters

The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter

- Select the frame where the change should take effect
  - Select **Set Subsequent Decoder Parameters...** from the **Options** menu, and make the needed changes. You can also right-click on the frame to select the same option.

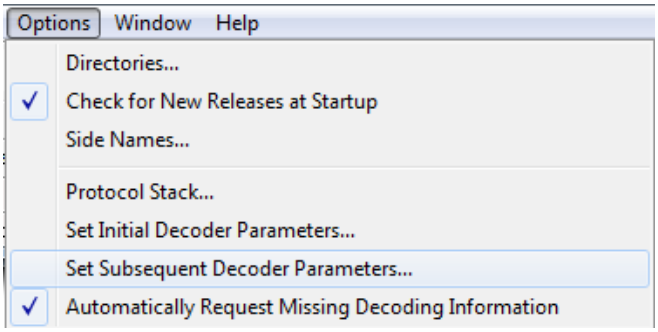


Figure 3.3 - **Set Subsequent Decoder Parameters...** from **Control** window

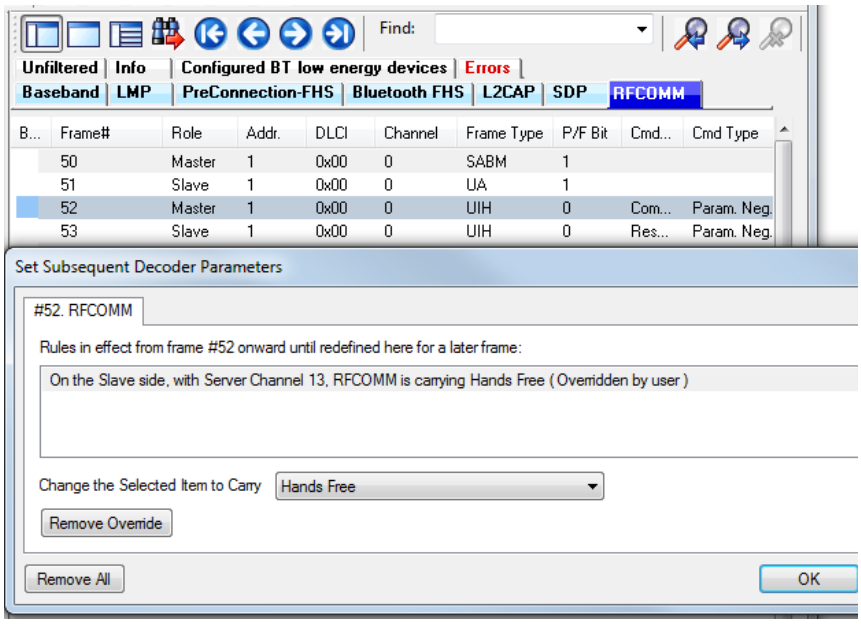


Figure 3.4 - Example: Set Subsequent Decode for Frame #52, RFCOMM

- Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.
- The **Remove Override** button will remove the selected decode parameter override.
- The **Remove All** button will remove all decoder overrides.

If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

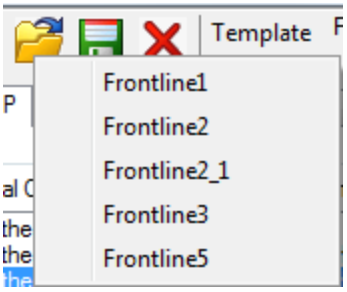
3.2.1 Decoder Parameter Templates

3.2.1.1 Select and Apply a Decoder Template

1. Select **Set Initial Decoder Parameters...** from the **Options** menu on the **Control** window or the **Frame Display**

window.

2. Click the **Open Template** icon in the toolbar and select the desired template from the pop up list. The system displays the content of the selected template in the Initial Connections list at the top of the dialog



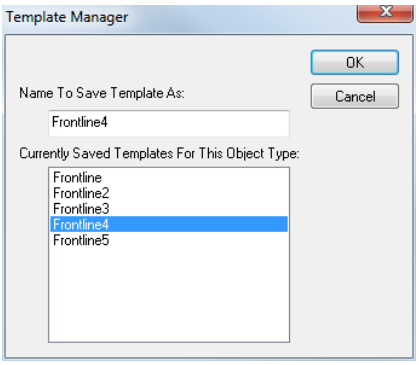
3. Click the OK button to apply the selected template and decoders' settings and exit the **Set Initial Decoder Parameters** dialog.

3.2.1.2 Adding a New or Saving an Existing Template

Add a Template

A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the **Save** button at the top of the **Set Initial Decoder Parameters** dialog to display the **Template Manager** dialog.



2. Enter a name for the new template and click **OK**.

   The system saves the template and closes the **Template Manager** dialog.

3. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the template and close the dialog.

Save Changes to a Template

This procedure saves changes to parameters in an existing template.

1. After making changes to parameter settings in a user defined template, click the **Save** button at the top of the **Set Initial Decoder Parameters** window to display the **Template Manager** dialog.
2. Ensure that the name of the template is listed in the **Name to Save Template As** text box and click **OK**.
3. The system displays a dialog asking for confirmation of the change to the existing template. Click the **Yes** button.

   The system saves the parameter changes to the template and closes the Save As dialog.

4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the template and close the window.

3.2.1.3 Deleting a Template

1. After opening the **Set Initial Decoder Parameters** window click the **Delete** button in the toolbar.

   The system displays the **Template Manager** dialog with a list of saved templates.

2. Select (click on and highlight) the template marked for deletion and click the **Delete** button.

   The system removes the selected template from the list of saved templates.

3. Click the **OK** button to complete the deletion process and close the Delete dialog.
4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the deletion and close the dialog.

3.2.2 Selecting A2DP Decoder Parameters

Decoding SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame. You can increase the decoding speed by decoding only the header fields and disregarding other parts. You can select the detail-level of decoding using the **Set Initial Decoder Parameters** window.

Note: By default the decoder decodes only the header fields of the frame.

1. Select **Set Initial Decoder Parameters** from the **Options** menu on the **Control** window or the **Frame Display** window.
2. Click on the **A2DP** tab.
3. Choose the desired decoding method.

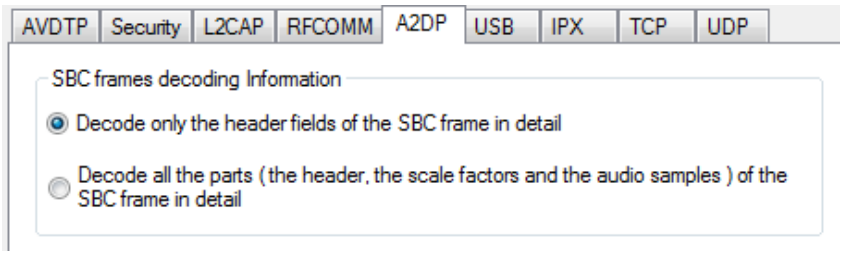


Figure 3.5 - A2DP Decoder Settings

4. Follow steps to save the template changes or to save a new template.
5. Click the **OK** button to apply the selection and exit the **Set Initial Decoder Parameters** window.

3.2.3 AVDTP Decoder Parameters

3.2.3.1 About AVDTP Decoder Parameters

Each entry in the **Set Initial Decoder Parameters** window takes effect from the beginning of the capture onward or until redefined in the **Set Subsequent Decoder Parameters** window.

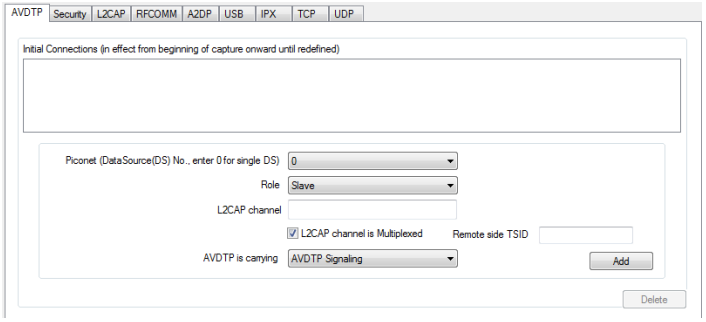


Figure 3.6 - AVDTP parameters tab

The **AVDTP** tab requires the following user inputs to complete a parameter:

- **Piconet (Data Source (DS) No.)** - When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired number of data sources.
- **Role** - This identifies the role of the device initiating the frame (**Master** or **Slave**)
- **L2CAP Channel** - The channel number 0 through 78.
  - **L2CAP channel is Multiplexed** - when checked indicates that L2CAP is multiplexed with upper layer protocols.
- **AVDTP is carrying** - Select the protocol that AVDTP traverses to from the following:
  - AVDTP Signaling
  - AVDTP Media
  - AVDTP Reporting
  - AVDTP Recovery
  - -Raw Data-

Adding, Deleting, and Saving AVDTP Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **AVDTP** tab.
2. Set or select the **AVDTP** decoder parameters.
3. Click on the **ADD** button. The Intial Connection window displays the added parameters.

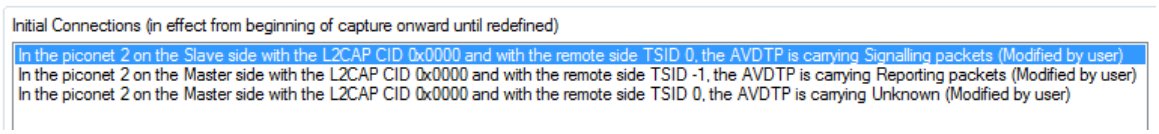

Initial Connections (in effect from beginning of capture onward until redefined)
In the piconet 2 on the Slave side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Signalling packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID -1, the AVDTP is carrying Reporting packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Unknown (Modified by user)

Figure 3.7 - Parameters Added to Decoder

4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.

5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.

6. AVDTP parameters are saved when the template is saved as described in Adding a New or Saving an Existing Template on page 41Adding a New or Saving an Existing Template on page 41

3.2.3.2 AVDTP Missing Decode Information

The analyzer usually determines the protocol carried in an AVDTP payload by monitoring previous traffic. However, when this fails to occur, the **Missing Decoding Information Detected** dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- The capture session started after transmission of the vital information.
- The analyzer incorrectly received a frame with the traversal information.
- The communication monitored takes place between two players with implicit information not included in the transmission.

In any case, either view the AVDTP payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note: You may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown “data” in the **Decoder** pane on the **Frame Display**. You may notice something that hints as to the profile in use.

In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

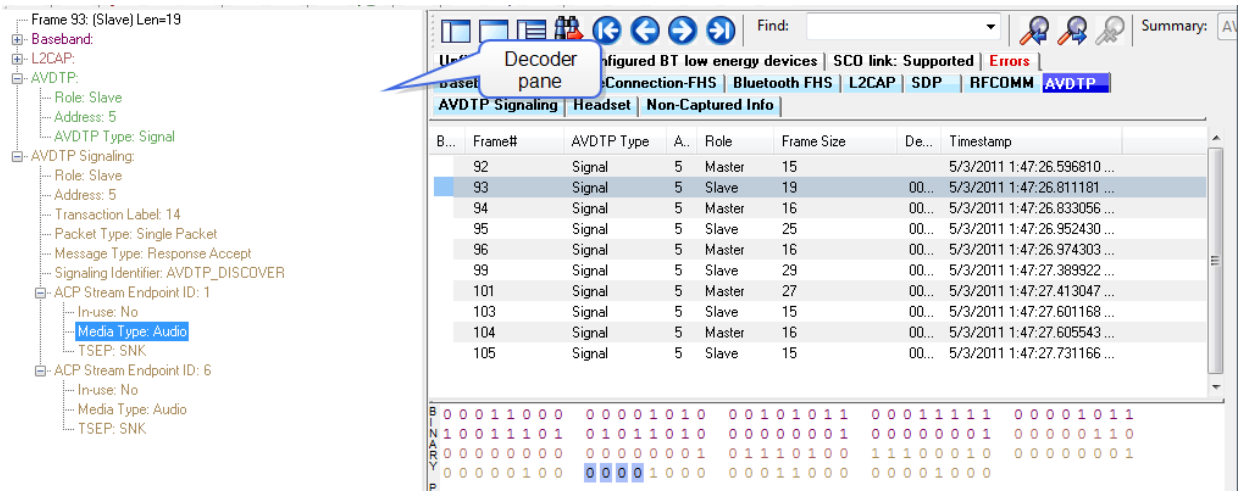

Frame 93: (Slave) Len=19
Baseband:
L2CAP:
AVDTP:
Role: Slave
Address: 5
AVDTP Type: Signal
AVDTP Signaling:
Role: Slave
Address: 5
Transaction Label: 14
Packet Type: Single Packet
Message Type: Response Accept
Signaling Identifier: AVDTP_DISCOVER
ACP Stream Endpoint ID: 1
In-use: No
Media Type: Audio
TSEP: SNK
ACP Stream Endpoint ID: 6
In-use: No
Media Type: Audio
TSEP: SNK
Decoder pane
Find:
Summary:
SCO link: Supported
Errors
L2CAP
SDP
RFCOMM
AVDTP
AVDTP Signaling
Headset
Non-Captured Info
Frame#
AVDTP Type
Role
Frame Size
Timestamp
92 Signal 5 Master 15 5/3/2011 1:47:26.596810
93 Signal 5 Slave 19 5/3/2011 1:47:26.811181
94 Signal 5 Master 16 5/3/2011 1:47:26.833056
95 Signal 5 Slave 25 5/3/2011 1:47:26.952430
96 Signal 5 Master 16 5/3/2011 1:47:26.974303
99 Signal 5 Slave 29 5/3/2011 1:47:27.389922
101 Signal 5 Master 27 5/3/2011 1:47:27.413047
103 Signal 5 Slave 15 5/3/2011 1:47:27.601168
104 Signal 5 Master 16 5/3/2011 1:47:27.605543
105 Signal 5 Slave 15 5/3/2011 1:47:27.731166
BINARY
0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 1 1 0 0 0 1 1 1 1 1 0 0 0 0 1 0 1 1
1 0 0 1 1 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 1 1 1 0 0 0 1 0 0 0 0 0 0 0 0 1
0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1 0 0 0

Figure 3.8 - Look in Decoder pane for profile hints

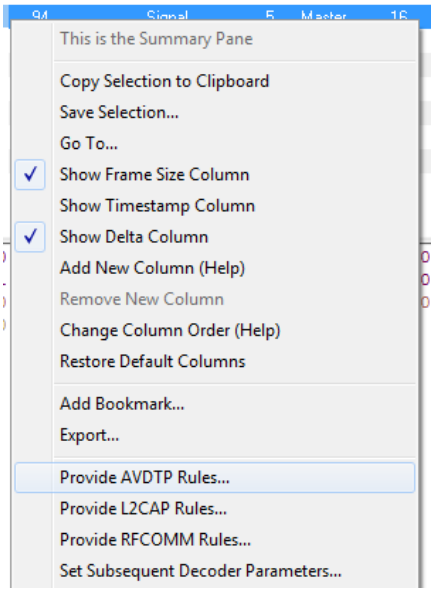
3.2.3.3 AVDTP Override Decode Information

The Set **Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect.
2. Select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
3. Select the rule you wish to modify from the list of rules.
4. Choose the protocol the selected item carries from the drop-down list, and click **OK**.

If you do not have any previously overridden parameters, you may set parameters for the current frame and onwards by right-clicking the desired frame and choosing **Provide AVDTP Rules...** from the right-click pop-up menu.



If you have a parameter in effect and wish to change it, there are two parameters that may be overridden for AVDTP: **Change the Selected Item to Carry**, and if AVDTP Media is selected. the codec type. Because there are times when vital AVDTP configuration information may not be transferred over the air, we give users the ability to choose between the four AVDTP channel types for each L2CAP channel carrying AVDTP as well as codec type. We attempt to make our best guess at codec information when it is not transferred over the air, but we realize we may not always be correct. When we make a guess for codec type, we specify it in the summary and decode panes by following the codec with the phrase '(best guess by analyzer). This is to let you know that this information was not obtained over the air and that the user may wish to alter it by overriding AVDTP parameters.

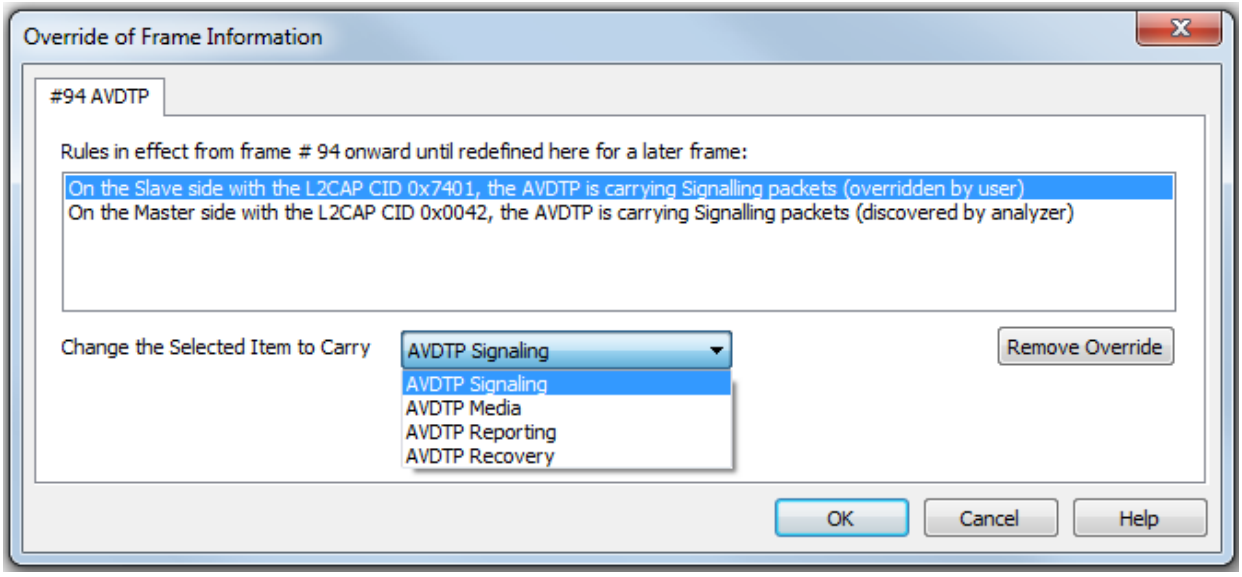

Override of Frame Information
#94 AVDTP
Rules in effect from frame # 94 onward until redefined here for a later frame:
On the Slave side with the L2CAP CID 0x7401, the AVDTP is carrying Signalling packets (overridden by user)
On the Master side with the L2CAP CID 0x0042, the AVDTP is carrying Signalling packets (discovered by analyzer)
Change the Selected Item to Carry
AVDTP Signaling
AVDTP Signaling
AVDTP Media
AVDTP Reporting
AVDTP Recovery
Remove Override
OK
Cancel
Help

Figure 3.9 - AVDTP Override of Frame Information, Item to Carry

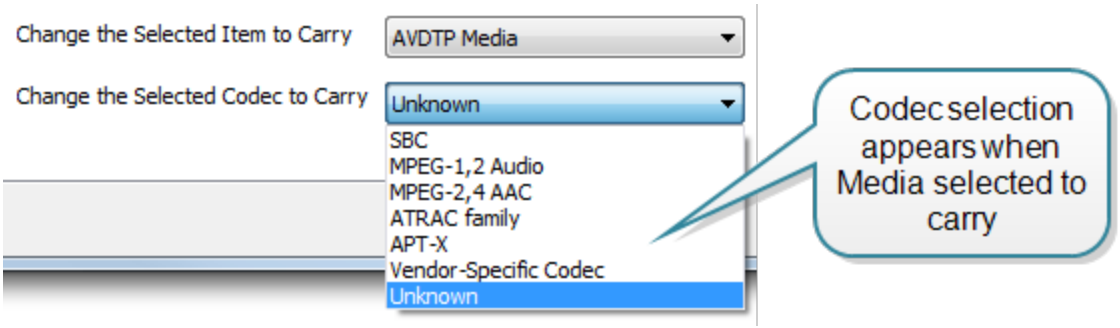
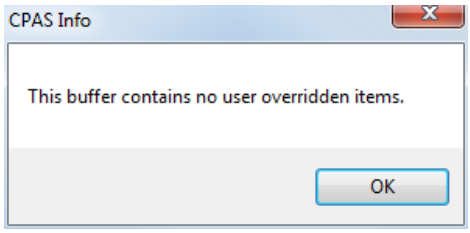


Figure 3.10 - AVDTP Override of Frame Information, Media Codec Selection

Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame. If you are unhappy with your changes, you can undo them by simply choosing your override from the dialog box and pressing the 'Remove Override' button. After pressing 'OK,' the capture file will recompile as if your changes never existed, so feel free to experiment with desired changes if you are unsure of what configuration to use.



Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.2.4 L2CAP Decoder Parameters

3.2.4.1 About L2CAP Decoder Parameters

Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

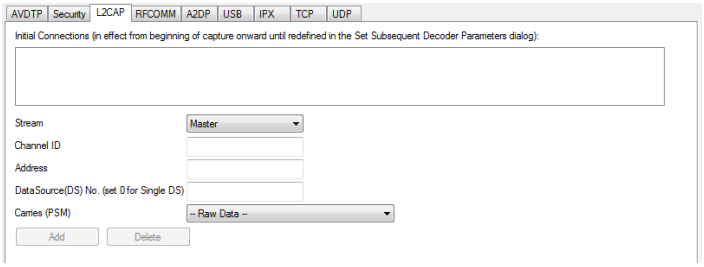
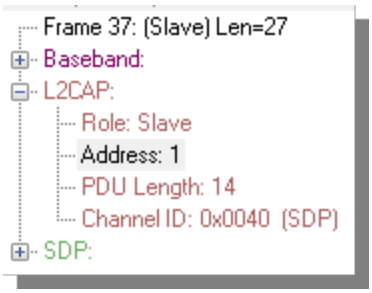


Figure 3.11 - L2CAP Decoder parameters tab

The **L2CAP Set Initial Decoder Parameters** dialog requires the following user inputs to complete a Parameter :

- **Stream** - This identifies the role of the device initiating the frame (master or slave)
- **Channel ID** - The channel number 0 through 78
- **Address** - This is the physical connection values for the devices. Each link in the net will have an address. A piconet can have up to seven links. The **Frame Display** can provide address information.



- **Data Source (DS) No.** -When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source number.

Carries (PSM) - Select the protocol that L2CAP traverses to from the following:

- AMP Manager
- AMP Test Manager
- SDP
- RFCOMM
- TCS
- LPMP
- BNEP
- HCRP Control
- HCRP Data
- HID

- AVCTP
- AVDTP
- CMTP
- MCAP Control
- IEEE P11073 20601
- -Raw Data-

Adding, Deleting, and Saving L2CAP Parameters

1. From the **Set Initial Decoder Parameters** window, click on the **L2CAP** tab.
2. Set or select the **L2CAP** decoder parameters.
3. Click on the **ADD** button. The Intial Connection window displays the added parameters.

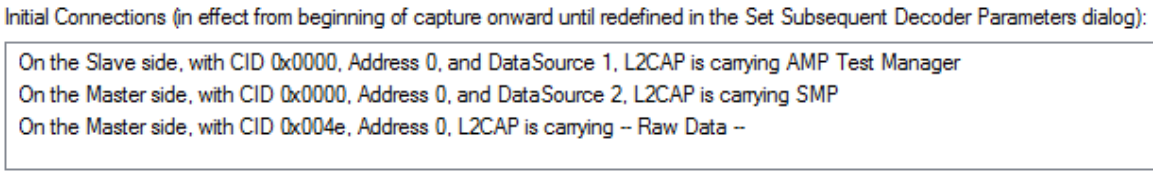

Initial Connections (in effect from beginning of capture onward until redefined in the Set Subsequent Decoder Parameters dialog):
On the Slave side, with CID 0x0000, Address 0, and DataSource 1, L2CAP is carrying AMP Test Manager
On the Master side, with CID 0x0000, Address 0, and DataSource 2, L2CAP is carrying SMP
On the Master side, with CID 0x004e, Address 0, L2CAP is carrying -- Raw Data --

Figure 3.12 - Parameters Added to Decoder

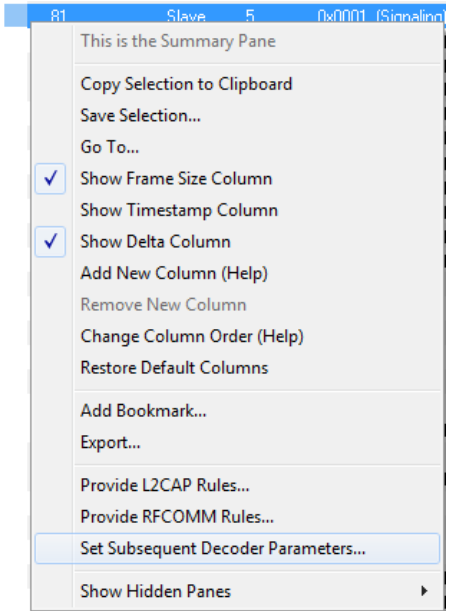
4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.
6. **L2CAP** parameters are saved when the template is saved. Adding a New or Saving an Existing Template on page 41

3.2.4.2 L2CAP Override Decode Information

The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect
2. Select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes. Refer to
3. Change the L2CAP parameter by selecting from the rule to change, and click on the listed parameters.
4. If you wish to remove an overridden rule click on **Remove Override** button. If you want to remove all decoder parameter settings click on **Remove All**.
5. Click **OK**.



Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

3.2.5 RFCOMM Decoder Parameters

3.2.5.1 About RFCOMM Decoder Parameters

Each entry in the **Set Initial Decoder Parameters** dialog takes effect from the beginning of the capture onward or until redefined in the **Set Subsequent Decoder Parameters** dialog.

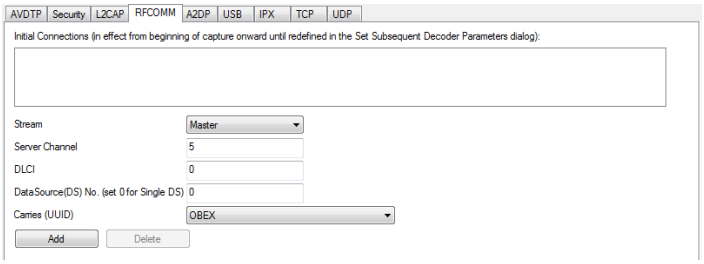

AVDTP Security L2CAP RFCOMM A2DP USB IPX TCP UDP
Initial Connections (in effect from beginning of capture onward until redefined in the Set Subsequent Decoder Parameters dialog):
Stream Master
Server Channel 5
DLCI 0
DataSource(DS) No. (set 0 for Single DS) 0
Carries (UUID) OBEX
Add
Delete

Figure 3.13 - RFCOMM parameters tab

The **RFCOMM Set Initial Decoder Parameters** tab requires the following user inputs to complete a parameter:

- **Stream** - Identifies the role of the device initiating the frame (master or slave)
- **Server Channel** - The Bluetooth® channel number 0 through 78
- **DLCI** - This is the Data Link Connection Identifier, and identifies the ongoing connection between a client and a server

- **Data Source (DS) No**.- When only one data source is employed, set this parameter to 0 (zero), otherwise, set to the desired data source
- **Carries (UUID)** - Select from the list to apply the Universal Unique Identifier (UUID) of the application layer that RFCOMM traverses to from the following:
    - OBEX
    - SPP
    - encap asyncPPP
    - Headset
    - FAX
    - Hands Free
    - SIM Access
    - VCP
    - UDI
    - -Raw Data-

Adding, Deleting, and Saving RFCOMMParameters

1. From the **Set Initial Decoder Parameters** window, click on the **RFCOMM**tab.
2. Set or select the **RFCOMM**decoder parameters.
3. Click ont he **ADD** button. The Intial Connection window displays the added parameters.

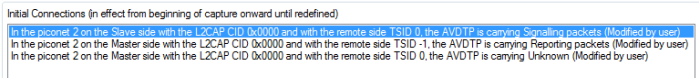

Initial Connections (in effect from beginning of capture onward until redefined)
In the piconet 2 on the Slave side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Signaling packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID -1, the AVDTP is carrying Reporting packets (Modified by user)
In the piconet 2 on the Master side with the L2CAP CID 0x0000 and with the remote side TSID 0, the AVDTP is carrying Unknown (Modified by user)

Figure 3.14 - Parameters Added to Decoder

4. To delete a parameter from the **Initial Connections** window, select the parameter and click on the **Delete** button.
5. Decoder parameters cannot be edited. The only way to change a parameter is to delete the original as described above, and recreate the parameter with the changed settings and selections and then click on the **Add** button.
6. RFCOMM parameters are saved when the template is saved as described in Adding a New or Saving an Existing Template on page 41

3.2.5.2 RFCOMM Missing Decode Information

ComProbe software usually determines the protocol carried in an RFCOMM payload by monitoring previous traffic. However, when this fails to occur, the **Missing Decoding Information Detected** dialog appears and requests that the user supply the missing information.

The following are the most common among the many possible reasons for a failure to determine the traversal:

- The capture session started after transmission of the vital information
- The analyzer incorrectly received a frame with the traversal information
- The communication monitored takes place between two players with implicit information not included in the transmission

In any case, either view the RFCOMM payload of this frame (and other frames with the same channel) as hex data, or assist the analyzer by selecting a protocol using this dialog.

Note that you may use the rest of the analyzer without addressing this dialog. Additional information gathered during the capture session may help you decide how to respond to the request for decoding information.

If you are not sure of the payload carried by the subject frame, look at the raw data shown under **data** in the **Decode** pane in the **Frame Display**. You may notice something that hints as to the profile in use.

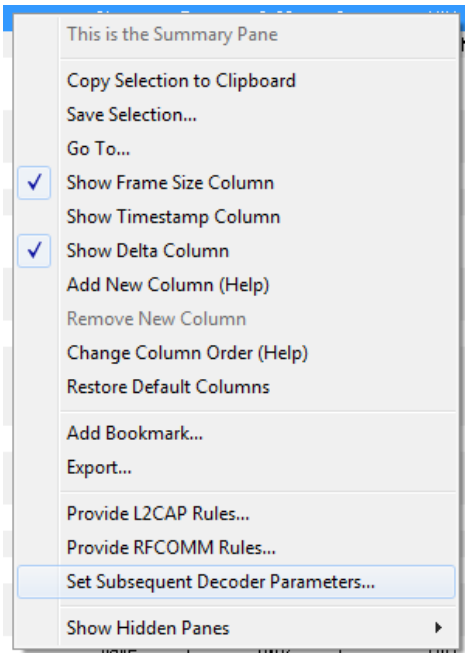
In addition, look at some of the frames following the one in question. The data may not be recognizable to the analyzer at the current point due to connection setup, but might be discovered later on in the capture.

3.2.5.3 RFCOMM Override Decode Information

The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter:

1. Select the frame where the change should take effect, and select **Set Subsequent Decoder Parameters** from the **Options** menu, or by selecting a frame in the frame display and choosing from the right-click pop-up menu, and make the needed changes.
2. Change the RFCOMM parameter by selecting from the **Change the Selected Item to Carry** drop down list.
3. If you wish to remove an overridden rule click on **Remove Override** button. If you want to remove all decoder parameter settings click on **Remove All**.
4. Choose the protocol the selected item carries from the drop-down list, and click **OK**.



Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

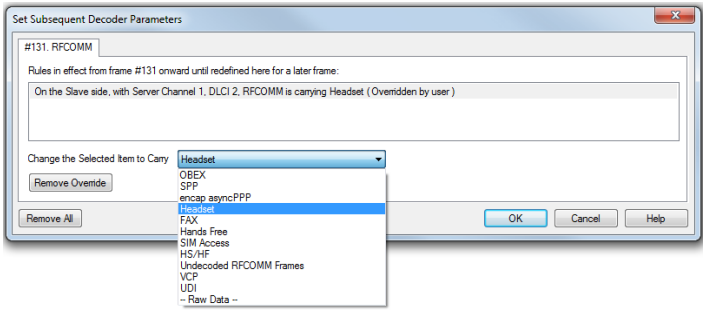


Figure 3.15 - Set Subsequent Decoder Parameters selection list

Note: If the capture has no user defined overrides, then the system displays a dialog stating that no user defined overrides exist.

Chapter 4 Capturing and Analyzing Data

The following sections describe the various ComProbe software functions that capture and display data packets.

4.1 Capture Data

4.1.1 Air Sniffing: Positioning Devices

When capturing over the air packets, proper positioning of the ComProbe hardware and the Devices Under Test (DUTs) will result in the best possible captures and will mitigate sources of path loss and interference. The following procedures will help optimize the capture process especially if you are have problems obtaining reliable …captures.

Problems with indoor radio propagation

Even in free space, it is well understood that radio frequencies attenuate over distance. The free-space rule-of-thumb dictates that radio energy decreases in strength by 20 dB by each 10-to-1 increase in range. In the real-world, the effects of objects in an outdoor environment cause reflection, diffraction, and scattering resulting in greater signal losses. Indoors the situation can be worse. Reflections occur from walls and other large flat surfaces. Diffraction occurs from objects with sharp edges. Scattering is produced from objects with rough surfaces and from small objects. Also any object directly in the path of the radiation can present a hard or soft partition depending on the partition's material properties. Path losses from partitions are difficult to estimate.

Estimating indoor propagation loss

One estimate of indoor path loss, based on path loss data from a typical building, provides a $\frac{1}{range^{3.5}}$ power rule. At 2.4 GHz, the following relationship provides an approximate estimate of indoor path loss:

$$Indoor\ Path\ Loss\ (in\ dB) = 40 + 35Log_{10}(range,\ in\ meters)$$

This approximation is expected to have a variance of 13 dB.

Mitigating path loss and interference

Bluetooth device design contributes to mitigating environmental effects on propagation through spread spectrum radio design, for example. However, careful planning of the testing environment can also contribute to reliable data capture process.

The first step to ensuring reliable air-sniffing data capture is to understand the RF characteristics of the Devices Under Test (DUTs). The *Bluetooth* Class, antenna types, and radiation patterns are all important factors that can affect the placement of the DUTs and the ComProbe analyzer. Radiation patterns are rarely spherical, so understanding your device's radiation patterns can greatly enhance successful data capture. Position devices to avoid radiation attenuation by the surroundings.

This step is optional: Consider conductive testing to establish a baseline capture. Conductive testing isolates the DUTs and analyzer from environmental effects.

The next step is to ensure that the testing environment is as clutter-free as possible.

- Line-of-sight obstructions should be eliminated between the ComProbe hardware and the DUTs because they cause a reduction in signal strength. Obstructions include, but are not limited to: water bottles, coffee cups, computers, computer screens, computer speakers, and books. A clear, unobstructed line-of-sight is preferred for DUT and ComProbe hardware positioning.
- If using an analyzer connected to a computer, position the computer on an adjacent table or surface away from the analyzer and DUTs, taking advantage of the cables' length. If this is not possible, position the computer behind the analyzer as far away as possible. If using the ComProbe FTS4BT, which is a dongle, either use an extension USB cable or position the computer such that the dongle is positioned towards the DUTs.
- The preferred placement is positioning the DUTs and the ComProbe hardware at the points of an equilateral triangle in the same horizontal plane, i.e. placed on the same table or work surface. The sides of the triangle should be between 1 and 2 meters for Bluetooth transmitter classes 1 and 2. The distance for transmitter class 3 should be 1/2 meter.

Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

- Wi-Fi interference should be minimized or eliminated. *Bluetooth* shares the same 2.4 GHz frequency bands as Wi-Fi technology. Wi-Fi interference can cause loss of packets and poor captures. In a laboratory or testing

environment do not place the DUTs and ComProbe hardware in close proximity with Wi-Fi transmitting sources such as laptops or routers. Turning off Wi-Fi on the computer running the ComProbe software is recommended.

Positioning for audio capture

The Bluetooth Audio Expert System provides analysis of audio streams and can assist in identifying problems with capture methods including positioning and environment because it will point out missing frames. For hands-free profile data captures both DUTs send and receive data. Therefore, position the devices following the equilateral triangle arrangement as mentioned above.

However, in A2DP data capture scenario, the equilateral positioning of devices is not optimum because, normally, only one device is sending data to the other. It is recommended that the ComProbe hardware be positioned closer to the device receiving data so that ComProbe better mimics the receiving DUT. Position the DUTs 1 -2 meters apart for Class 1 and 2 transmitters, and 1/2 meter apart for Class 3 transmitters.

Figure 4.2 - For Audio A2DP, Position Closer to SINK DUT

Poor Placement

A poor test configuration for the analyzer is placing the DUTs very close to each other and the analyzer far away. The DUTs, being in close proximity to each other, reduce their transmission power and thus make it hard for the analyzer to hear the conversation. If the analyzer is far away from DUTs, there are chances that the analyzer may miss those frames, which could lead to failure in decryption of the data.

Obstacles in close proximity to or in between the analyzer and the DUTs can interfere and cause reduction in signal strength or interference. Even small objects can cause signal scattering.

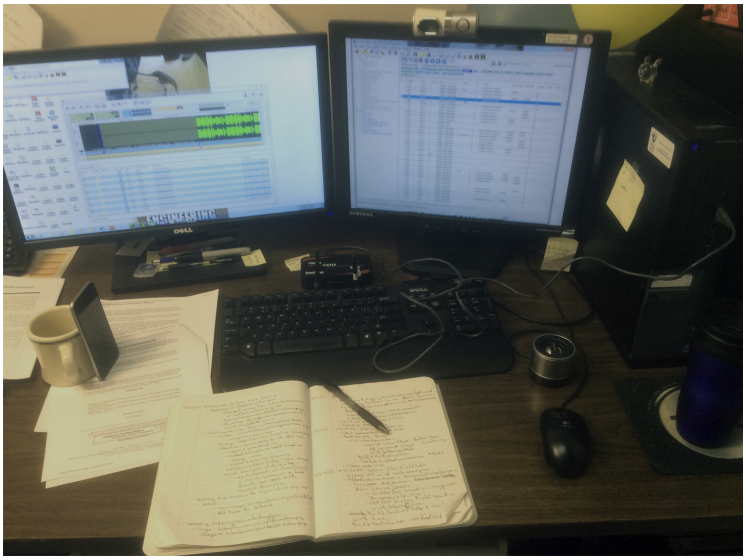


Figure 4.3 - Example: Poor Capture Environment

4.1.2 Capturing Data to Disk - General Procedure

Note: Capture is not available in Viewer mode.

1. Click the **Start Capture** button to begin capturing to a file. This icon is located on the **Control** , **Event Display**, and **Frame Display** windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose **Directories** from the **Options** menu on the **Control** window to change the default file location.

   Note: For the Dashboard, when you capture to series of files, the window displays the data from the beginning of the first capture, even when a new file in the series is created. This is because the Dashboard is a "Session Monitor", which means that even if you capture to a series of files, the data from the first file is always displayed. The display does not refresh when a new capture file in a series is created.
3. Watch the status bar on the **Control** window to monitor how full the file is. When the file is full, it begins to **wrap**, which means the oldest data will be overwritten by new data.
4. Click the **Stop Capture** icon to temporarily stop data capture. Click the **Start Capture** icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured data remains in the file.
5. To clear captured data, click the **Clear** icon .

   - If you select **Clear** after selecting **Stop Capture**, a dialog appears asking whether you want to save the data.

- You can click **Save File** and enter a file name when prompted .
- If you choose **Do Not Save**, all data will be cleared.
- If you choose **Cancel,** the dialog closes with no changes.

- If you select the **Clear** icon while a capture is occurring:
  - The capture stops.
  - A dialog appears asking if you want to save the capture
  - You can select **Yes** and save the capture or select **No** and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
  - If you choose **Cancel**, the dialog closes with no changes.

To see how to capture to a single file, choose System Settings from the Options menu on the Control window.

When live capture stops, no new packets are sniffed but there can still be packets that were previously sniffed but not yet read by the ComProbe analyzer. This happens when packets are being sniffed faster than the ComProbe analyzer can process them. These packets are stored either on the ComProbe hardware itself or in a file on the PC. If there are remaining packets to be processed when live capture stops the **Transferring Packets** dialog below is displayed showing the packets yet to be read by the ComProbe analyzer. The dialog shows the name of each ComProbe hardware device, its process id in square brackets, and the number of packets remaining. These stored packets are read until they're exhausted or the user clicks the Discard button on the dialog.

Unlike 802.11, *Bluetooth* packets never come in faster than the datasource can process them. However, *Bluetooth* packets must still be stored so that they can be read in chronological order with the 802.11 packets.

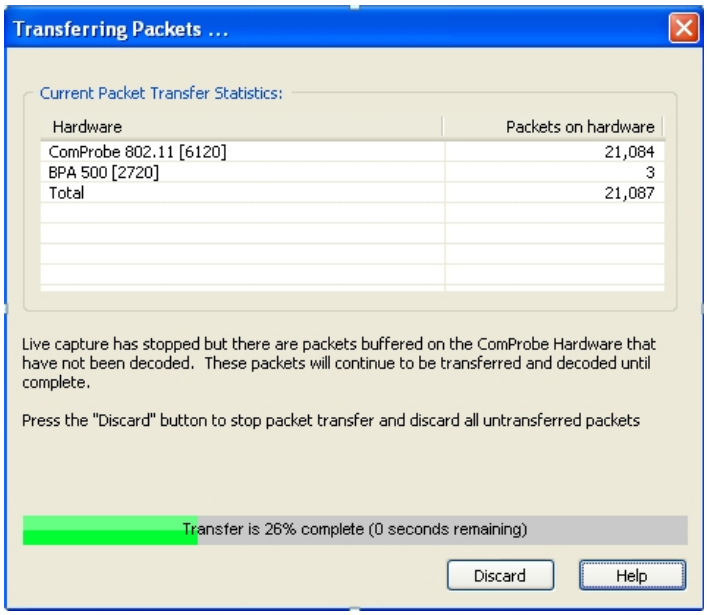

Transferring Packets ...
Current Packet Transfer Statistics:
Hardware
Packets on hardware
ComProbe 802.11 [6120]
21,084
BPA 500 [2720]
3
Total
21,087
Live capture has stopped but there are packets buffered on the ComProbe Hardware that have not been decoded. These packets will continue to be transferred and decoded until complete.
Press the "Discard" button to stop packet transfer and discard all untransferred packets
Transfer is 26% complete (0 seconds remaining)
Discard
Help

Figure 4.4 - Packet Transfer Dialog

4.1.3 Capturing Data with BPA 500 Devices

Once you have completed the **Devices Under Test** selection, you are ready to capture data.

Note: Data Capture is not available in Viewer mode.

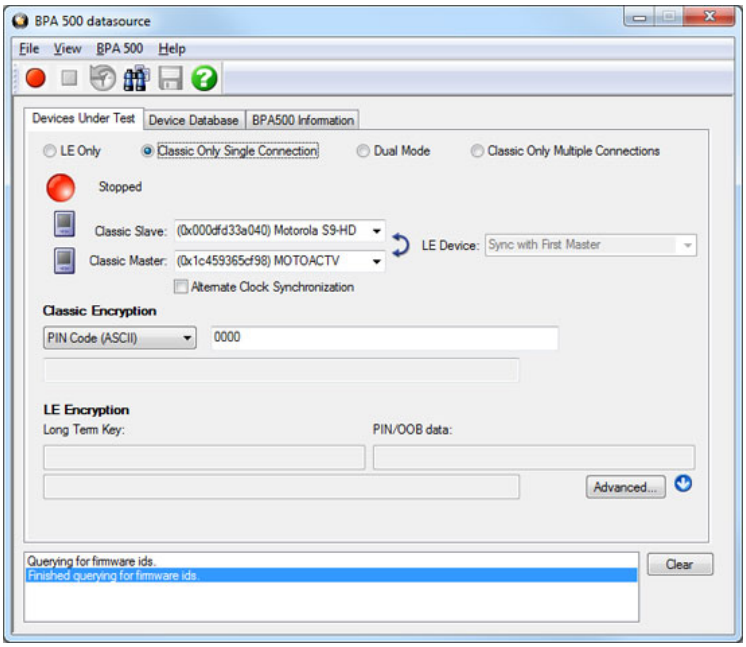


Figure 4.5 - BPA 500 Datasource Dialog

1. Select the start sniffing button on the toolbar or,**Start Sniffing** on the **BPA 500** menu.

2. The pairing process between the devices begins.

As data is being captured, the Status message at the top of the window indicates the synchronization status of the ComProbe analyzer. Also, the color of the ComProbe icon changes depending on the synchronization state. There are four states:

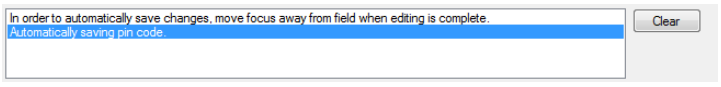
Table 4.1 - BPA 500 LED Capture Indicators

LED Color	Description
	Red = Halted/Pending
	Green = Waiting for the master to connect to the slave
	Blue = Synchronized with the master clock — link active
	Grey = Synchronized with the master clock — link inactive
	Yellow = Waiting for the master to resume transmission

When you are capturing data, there are several important concepts to consider.

- Files are placed in My Capture Files by default and have a .cfa extension. Choose **Directories** from the **Options** menu on the **Control** window to change the default file location.

- Watch the status bar on the **Control** window to monitor how full the file is. When the file is full, it begins to wrap, which means the oldest data will be overwritten by new data.
- Click the **Stop** icon to temporarily stop data capture. Click the **Start Capture** icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.
- To clear captured data, click the **Clear** icon .
    - If you select **Clear** after selecting **Stop**, a dialog appears asking whether you want to save the data.
        - You can click **Save File** and enter a file name when prompted .
        - If you choose **Do Not Save**, all data will be cleared.
        - If you choose **Cancel,** the dialog closes with no changes.
    - If you select the **Clear** icon while a capture is occurring:
        - The capture stops.
        - A dialog appears asking if you want to save the capture
        - You can select Yes and save the capture or select No and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
        - If you choose Cancel, the dialog closes with no changes.
- The link key/pin code can be changed while sniffing and the changes will be automatically saved in the configuration file.
    - While the device is sniffing click in the Classic Encryption link key/pin code field. This action places the focus on that window.
    - Change the link key/pin code.
    - The Status window at the bottom of the page will inform the user to move focus away from the link key/pin code window.
    - Click the mouse outside the link key/pin code field or press the Tab key. This action will remove the focus from the link key/pin code window.
    - The link key/pin code changes are automatically saved to the configuration file.


In order to automatically save changes, move focus away from field when editing is complete.
Automatically saving pin code.
Clear

4.1.4 Extended Inquiry Response

Extended Inquiry Response (EIR) is a tab that appears automatically on the **Frame Display** window when you capture data.

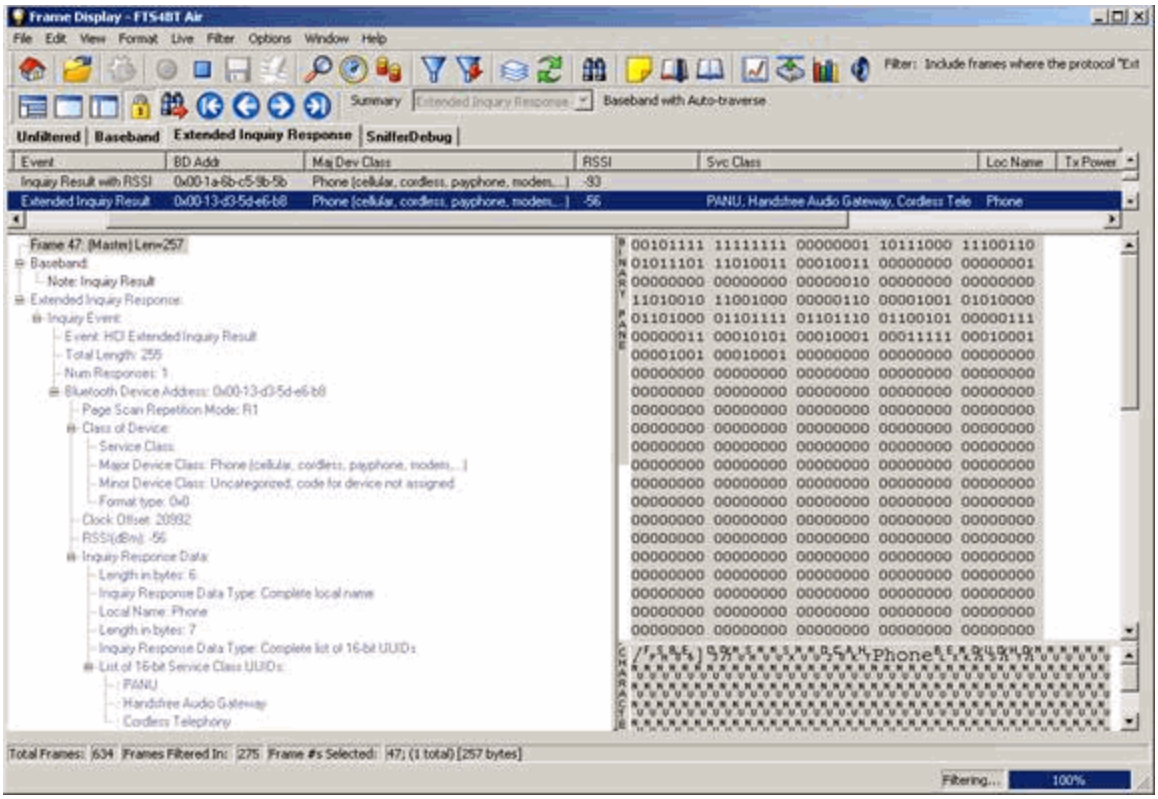

Frame Display - FTS4BT Air
File Edit View Format Live Filter Options Window Help
Unfiltered Baseband Extended Inquiry Response SnifferDebug
Event BD Addr Maj Dev Class RSSI Svc Class Loc Name Tx Power
Inquiry Result with RSSI 0x00-1a-6b-c5-9b-5b Phone (cellular, cordless, payphone, modem...) -93
Extended Inquiry Result 0x00-13-d3-5d-e6-b8 Phone (cellular, cordless, payphone, modem...) -56 PANU; Handsfree Audio Gateway; Cordless Tele Phone
Frame 47: (Master) Len=257
Baseband
Note: Inquiry Result
Extended Inquiry Response
Inquiry Event
Event: HCI Extended Inquiry Result
Total Length: 255
Num Responses: 1
Bluetooth Device Address: 0x00-13-d3-5d-e6-b8
Page Scan Repetition Mode: R1
Class of Device
Service Class:
Major Device Class: Phone (cellular, cordless, payphone, modem...)
Minor Device Class: Uncategorized, code for device not assigned
Format type: 0x0
Clock Offset: 20992
RSSI(dBm): -56
Inquiry Response Data
Length in bytes: 6
Inquiry Response Data Type: Complete local name
Local Name: Phone
Length in bytes: 7
Inquiry Response Data Type: Complete list of 16-bit UUIDs
List of 16-bit Service Class UUIDs:
PANU
Handsfree Audio Gateway
Cordless Telephony
Total Frames: 634 Frames Filtered In: 275 Frame #s Selected: 47; (1 total) [257 bytes]
Filtering... 100%

Figure 4.6 - Frame Display Extended Inquire Response

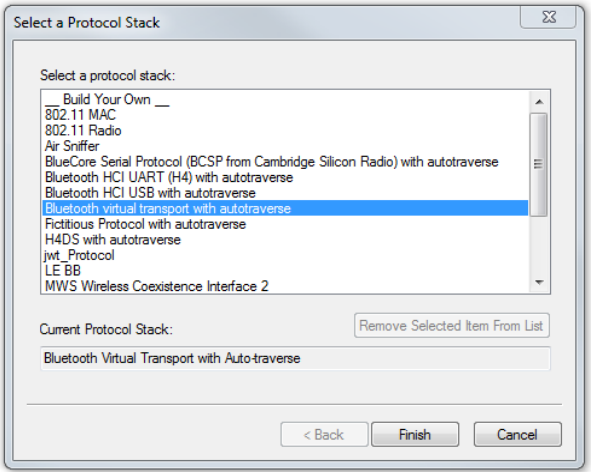
EIR displays extensive information about the Bluetooth® devices that are discovered as data is being captured. EIR provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode. Before the EIR tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be made to a device prior to making the connection.

Note: If a *Bluetooth* device does not support **Extended Inquiry Response**, the tab displays **Received Signal Strength Indication** (RSSI) data, which is less extensive than EIR data.

4.2 Protocol Stacks

4.2.1 Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.



To start the wizard:

1. Choose **Protocol Stack** from the **Options** menu on the **Control** window or click the **Protocol Stack** icon on the **Frame Display**.
2. Select a protocol stack from the list, and click **Finish**.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating and Removing a Custom Stack on page 62.

1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the **Remove Selected Item From List** button becomes active.
2. Click the **Remove Selected Item From List**button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

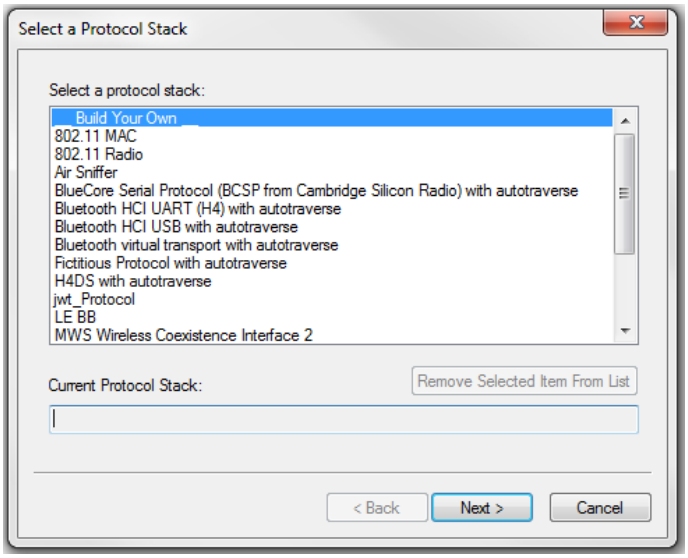
If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 63 for more information.

You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

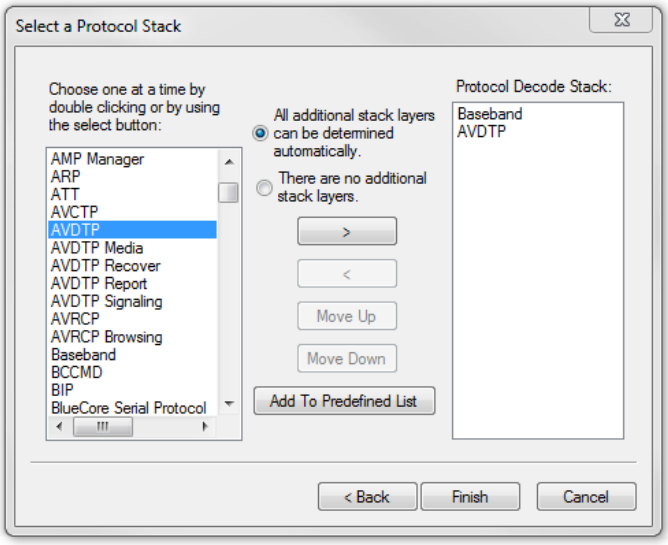
If you are using Modbus TCP over Ethernet, you need to set up a node database giving the IP addresses for the Master and Slave devices. for more information.

4.2.2 Creating and Removing a Custom Stack

To create a custom stack:



1. Choose **Protocol Stack** from the **Options** menu on the **Control** window or click the Protocol Stack icon on the **Frame Display** toolbar.
2. Select **Build Your Own** from the list and click **Next**.
3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click **Next** to continue.



Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the **Protocol Decode Stack** box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the **Move Up** and **Move Down** buttons until the protocol is in the correct position.
5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

Auto-traversal (Have the analyzer Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers:

1. Click the **All additional stack layers can be determined automatically** button.
2. If your protocol stack is complete and there are no additional layers, click the **There are no additional stack layers** button.

3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

1. Click the Add To Predefined List button.
2. Give the stack a name, and click Add.

In the future, the stack appears in the **Protocol Stack List** on the first screen of the Protocol Stack wizard.

Remove a Stack

1. Select it in the first screen and click Remove Selected Item From List.
2. If you remove the stack, you must to recreate it if you need to use it again.

Note: If you do not save your custom stack, it does appear in the predefined list, but applies to the frames in the current session. However, it is discarded at the end of the session.

4.2.3 Reframing

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. You can also use **Reframe** to frame unframed data. The original capture file is not altered during this process.

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To reframe your data, load your capture file, select a protocol stack, and then select **Reframe** from the **File** menu on the **Control** window. **Reframe** is only available if the frame recognizer used to capture the data is different from the current frame recognizer.

In addition to choosing to **Reframe**, you can also be prompted to Reframe by the Protocol Stack Wizard.

1. Load your capture file by choosing **Open** from the **File** menu on the **Control** window, and select the file to load.
2. Select the protocol stack by choosing **Protocol Stack** from the **Options** menu on the **Control** window, select the desired stack and click **Finish**.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the **Protocol Stack Wizard** asks you if you want to reframe your data. Choose **Yes**.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing on page 63 for instructions on removing framing from data.

4.2.4 Unframing

This function removes start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process. You cannot unframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To manually unframe your data:

1. Select **Unframe** from the **File** menu on the **Control** window. **Unframe** is only available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

In addition to choosing to **Unframe**, you can also be prompted to Unframe by the Protocol Stack Wizard.

1. Load your capture file by choosing **Open** from the **File** menu on the **Control** window.
2. Select the file to load.
3. Choose **Protocol Stack** from the **Options** menu on the **Control** window
4. Select **None** from the list
5. Click **Finish**. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file.
6. Choose **Yes**.

The system removes the frame markers from your data, puts the unframed data into a new file, and opens the new file. The original capture file is not altered.

See Reframing on page 63 for instructions on framing unframed data.

4.2.5 How the Analyzer Auto-traverses the Protocol Stack

In the course of doing service discovery, devices ask for and receive a Protocol Descriptor List defining which protocol stacks the device supports. It also includes information on which PSM to use in L2CAP, or the channel number for RFCOMM, or the port number for TCP or UDP. The description below talks about how the analyzer auto-traverses from L2CAP using a dynamically assigned PSM, but the principle is the same for RFCOMM channel numbers and TCP/UDP port numbers.

The analyzer looks for SDP Service Attribute Responses or Service Search Attribute Responses carrying protocol descriptor lists. If the analyzer sees L2CAP listed with a PSM, it stores the PSM and the UUID for the next protocol in the list.

After the SDP session is over, the analyzer looks at the PSM in the L2CAP Connect frames that follow. If the PSM matches one the analyzer has stored, the analyzer stores the source channel ID and destination channel ID, and associates those channel IDs with the PSM and UUID for the next protocol. Thereafter, when the analyzer sees L2CAP frames using those channel IDs, it can look them up in its table and know what the next protocol is.

In order for the analyzer to be able to auto-traverse using a dynamically assigned PSM, it has to have seen the SDP session giving the Protocol Descriptor Lists, and the subsequent L2CAP connection using the PSM and identifying the source and channel IDs. If the analyzer misses any of this process, it is not able to auto-traverse. It stops decoding at the L2CAP layer.

For L2CAP frames carrying a known PSM (0x0001 for SDP, for example, or 0x0003 for RFCOMM), the analyzer looks for Connect frames and stores the PSM along with the associated source and destination channel IDs. In this case the analyzer does not need to see the SDP process, but does need to see the L2CAP connection process, giving the source and destination channel IDs.

4.2.6 Providing Context For Decoding When Frame Information Is Missing

There may be times when you need to provide information to the analyzer because the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame

indicating the command.

The analyzer provides a way for you to supply the context for any frame, provided the decoder supports it. (The decoder writer has to include support for this feature in the decoder, so not all decoders support it. Note that not all decoders require this feature.)

If the decoder supports user-provided context, three items are active on the **Options** menu of the **Control** window and the **Frame Display** window. These items are **Set Initial Decoder Parameters**, **Automatically Request Missing Decoding Information**, and **Set Subsequent Decoder Parameters**. (These items are not present if no decoder is loaded that supports this feature.)

Set Initial Decoder Parameters is used to provide required information to decoders that is not context dependent but instead tends to be system options for the protocol.

Choose **Set Initial Decoder Parameters** in order to provide initial context to the analyzer for a decoder. A dialog appears that shows the data for which you can provide information.

If you need to change this information for a particular frame :

1. Right-click on the frame in the Frame Display window
2. Choose Provide <context name>.

Alternatively, you can choose **Set Subsequent Decoder Parameter** from the **Options** menu.

3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check **Automatically Request Missing Decoding Information.**
5. When unchecked, the analyzer doesn't bother you with dialogs asking for frame information that you don't have. In this situation, the analyzer decodes each frame until it cannot go further and then simply stop decoding.

4.3 Analyzing Byte Level Data

4.3.1 Event Display

To open this window click the **Event Display** icon on the **Control** window toolbar.

The **Event Display** window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and the analyzer information, such as when the data capture was paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

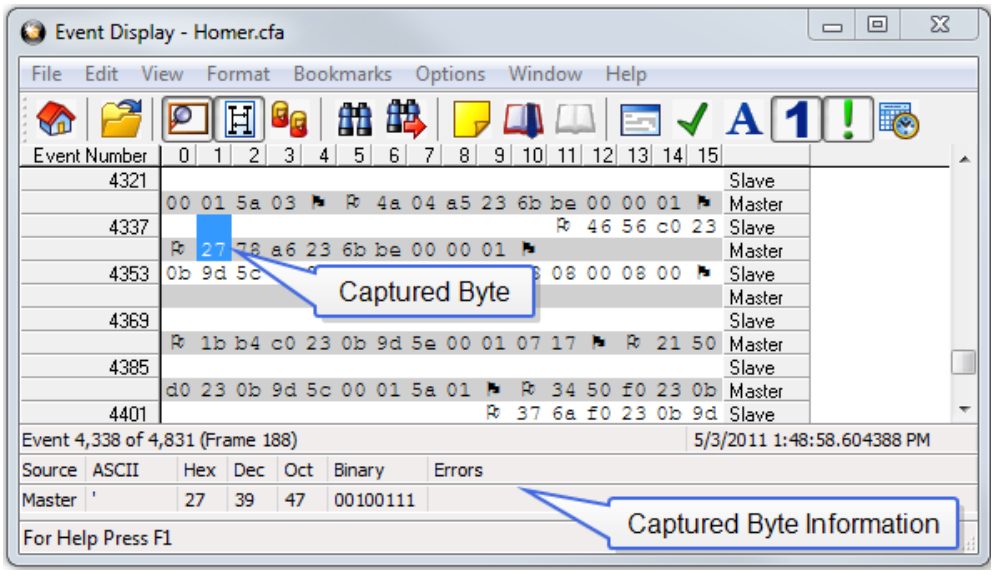

Event Display - Homer.cfa
File Edit View Format Bookmarks Options Window Help
Event Number
Captured Byte
Event 4,338 of 4,831 (Frame 188)
5/3/2011 1:48:58.604388 PM
Source ASCII Hex Dec Oct Binary Errors
Master ' 27 39 47 00100111
Captured Byte Information
For Help Press F1

Figure 4.2 Event Display

Click on an event to find out more about it. The three status lines at the bottom of the window are updated with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in hex, decimal, octal, and binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, the analyzer continually updates the Event Display as data is captured. Make sure the **Lock** icon is displayed on the toolbar to prevent the display from updating (Clicking on the icon again will unlock the display). While locked, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the **Lock** icon again.

You can have more than one **Event Display** open at a time. Click the **Duplicate View** icon to create a second, independent **Event Display** window. You can lock one copy of the **Event Display** and analyze your data, while the second **Event Display** updates as new data is captured.

Event Display is synchronized with the **Frame Display** and **Mesage Sequence Chart** dialogs. Selecting a byte in **Event Display** will also select the related frame in the **Frame Display** and the related message in the **Message Sequence Chart**.

4.3.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Home – Brings the Control window to the front.

Start Capture - Begins data capture to disk.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.

Clear- Discards the temporary file and clears the display.

MSC Chart - Opens the Message Sequence Chart

Lock - In the Lock state, the window is locked so you can review a portion of data. Data capture continues in the background. Clicking on the Lock icon unlocks the window.

Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon locks the window.

Duplicate View - Creates a second Event Display window identical to the first.

Frame Display - (framed data only) Brings up a Frame Display, with the frame of the currently selected bytes highlighted.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Find - Search for errors, string patterns, special events and more.

Go To - Opens the Go To dialog, where you can specify which event number to go to.

CRC - Change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC appears in the status lines at the bottom of the Event Display.

Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.

Character Only - The analyzer shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.

Number Only - Controls whether the analyzer displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.

All Events - Controls whether the analyzer shows all events in the window, or only data bytes. Events include control signal changes and framing information.

Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

4.3.3 Opening Multiple Event Display Windows

Click the **Duplicate View** icon from the **Event Display** toolbar to open a second **Event Display** window.

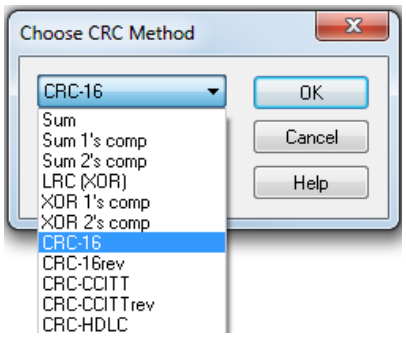
You can open as many **Event Display** windows as you like. Each **Event Display** is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The **Event Display** windows are numbered in the title bar. If you have multiple **Event Displays** open, click on the **Event Display** icon on the **Control** window toolbar to show a list of all the **Event Displays** currently open. Select a window from the list to bring it to the front.

4.3.4 Calculating CRCs or FCSs

The cyclic redundancy check (CRC) is a function on the **Event Display** window used to produce a checksum. The frame check sequence (FCS) are the extra checksum characters added to a frame to detect errors.

1. Open the **Event Display** window.
2. Click and drag to select the data for which you want to generate a CRC.
3. Click on the **CRC** icon .
4. In the **CRC** dialog box, click on the down arrow to show the list of choices for CRC algorithms..
5. Enter a **Seed** value in hexadecimal if desired.
6. Click **OK** to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC is calculated automatically.



4.3.5 Calculating Delta Times and Data Rates

1. Click on the E**vent Display** icon on the **Control** window to open the **Event Display** window.
2. Use the mouse to select the data you want to calculate a delta time and rate for.
3. The **Event Display** window displays the delta time and the data rate in the status lines at the bottom of the window.

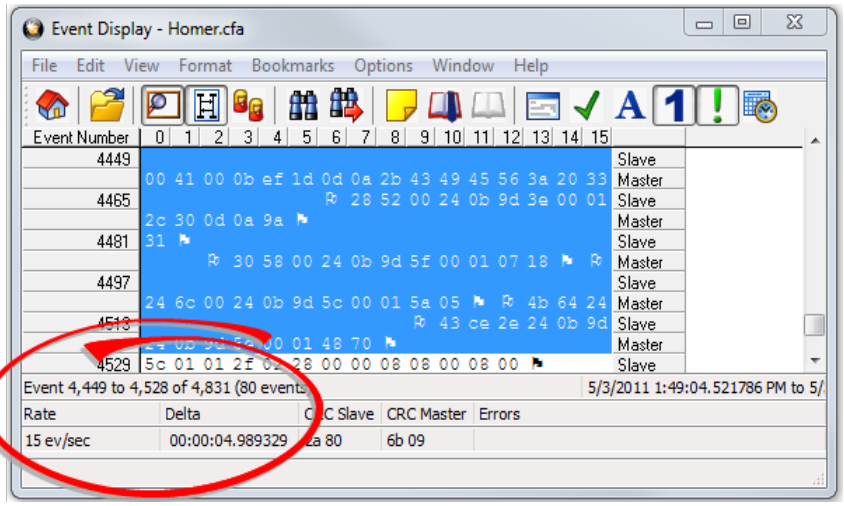


Figure 4.3 Delta fields

4.3.6 Switching Between Live Update and Review Mode

The **Event Display** and **Frame Display** windows can update to display new data during live capture, or be frozen to allow data analysis. By default, the **Event Display** continually updates with new data, and the **Frame Display** is locked.

1. Make sure the **Lock** icon is active so the display is locked and unable to scroll.

2. Click the **Unlock** icon again to resume live update.

The analyzer continues to capture data in the background while the display is locked. Upon resuming live update, the display updates with the latest data.

You can have more than one **Event Display** or **Frame Display** window open at a time. Click the **Duplicate View** icon to open additional Event or Frame Display windows. The lock/resume function is independent on each window. This means that you can have two **Event Display** windows open simultaneously, and one window can be locked while the other continues to update.

4.3.7 Data Formats and Symbols

4.3.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all **events**[1] that include:

- Data bytes
- Start-of-frame
- End-of-frame characters
- Data Captured Was Paused.

[1]An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.

Click on the **Display All Events** icon to remove the non-data events. Click again to display all events.

See List of all Event Symbols on page 72 for a list of all the special events shown in the analyzer and what they mean.

4.3.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the **radix**[1] used to display data.

Go to the **Format** menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.

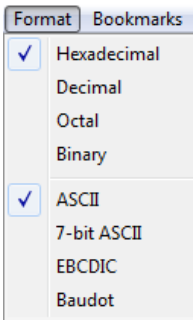


Figure 4.7 - Format Menu

1. Right-click on the data display header labels and choose a different radix.

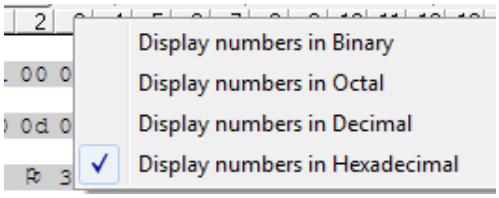


Figure 4.8 - Header labels, right click

2. Or right-click anywhere in the data display and select a different radix.

[1]The base of a number system. Binary is base 2, octal is base 8, decimal is base 10 and hexadecimal is base 16.

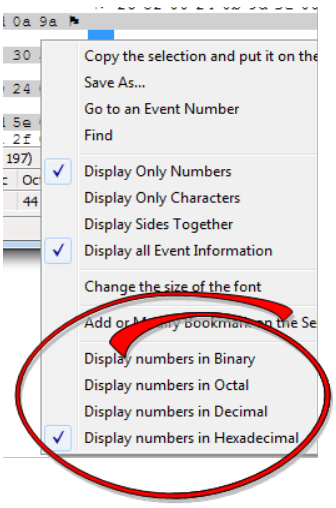


Figure 4.9 - Data display right click menu

If you want to see only the numerical values, click on the **Numbers Only** icon on the **Event Display** toolbar.

4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the **Event Display** window, the analyzer displays data in ASCII by default when you click on the **Characters Only** icon . There are several ways to change the character set used to display data.

1. Go to the **Format** menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. With the data displayed in characters, right-click on the data panel header label to choose a different character set.

If you want to see only characters, click on the Characters Only icon on the Event Display toolbar.

4.3.7.4 Selecting Mixed Channel/Sides

If you want to get more data on the **Event Display** window, you can switch to mixed sides mode. This mode puts all the data together on the same line. Data from one side (**Slave**) is shown on a white background and data from the other side (**Master**)is shown on a gray background.

1. Click once on the **Mixed Sides** icon to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click in the center of the data display window to change between mixed and side over side modes by selecting **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.
4. Right click in the sides panel on the right of the data display and select **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.

4.3.7.5 List of all Event Symbols

By default, the **Event Display** shows all events**events**[1], which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button . Click again to display all events.

Click on a symbol, and the analyzer displays the symbol name and sometimes additional information in the status lines at the bottom of the **Event Display** window. For example, clicking on a control signal change symbol displays which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

Table 4.4 - Event Symbols

Symbol	Event
	Abort
	Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.
	I/O Settings Change - A change was made in the I/O Settings window which altered the baud, parity, or other circuit setting.

[1]An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.

Table 4.4 - Event Symbols (continued)

Symbol	Event
	Long Break
	Low Power - The battery in the ComProbe® is low.
	Short Break
	SPY Event (SPY Mode only) - SPY events are commands sent by the application being spied on to the UART.
	Start of Frame - Marks the start of a frame.
	Begin Sync Character Strip
	End Sync Character Strip
	Sync Dropped
	Sync Found
	Sync Hunt Entered
	Sync Lost
	Test Device Stopped Responding - The analyzer lost contact with the ComProbe for some reason, often because there is no power to the ComProbe.
	Test Device Began Responding - The analyzer regained contact with the ComProbe.
	Timestamping Disabled - Timestamping was turned off. Events following this event are not timestamped.
	Timestamping Enabled - Timestamping was turned on. Events following this event have timestamps.
	Truncated Frame- A frame that is not the same size as indicated within its protocol.
	Underrun Error
	Unknown Event

4.3.7.6 Font Size

The font size can be changed on several **Event Display** windows. Changing the font size on one window does not affect the font size on any other window.

To change the font size:

1. Click on **Event Display** menu **Options,** and select **Change the Font Size**.

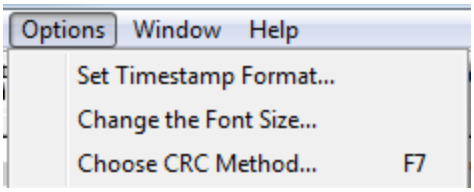


Figure 4.10 - Event Display Options menu

2. Choose a font size from the list.

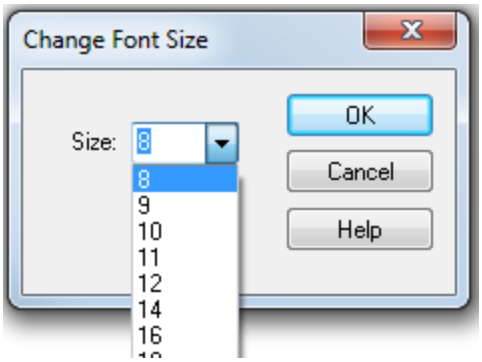


Figure 4.11 - Event Display Font Size Selection

3. Click **OK**.

4.4 Analyzing Protocol Decodes

4.4.1 Frame Display Window

To open this window

Click the **Frame Display** icon on the **Control** window toolbar, or select **Frame Display** from the **View** menu.

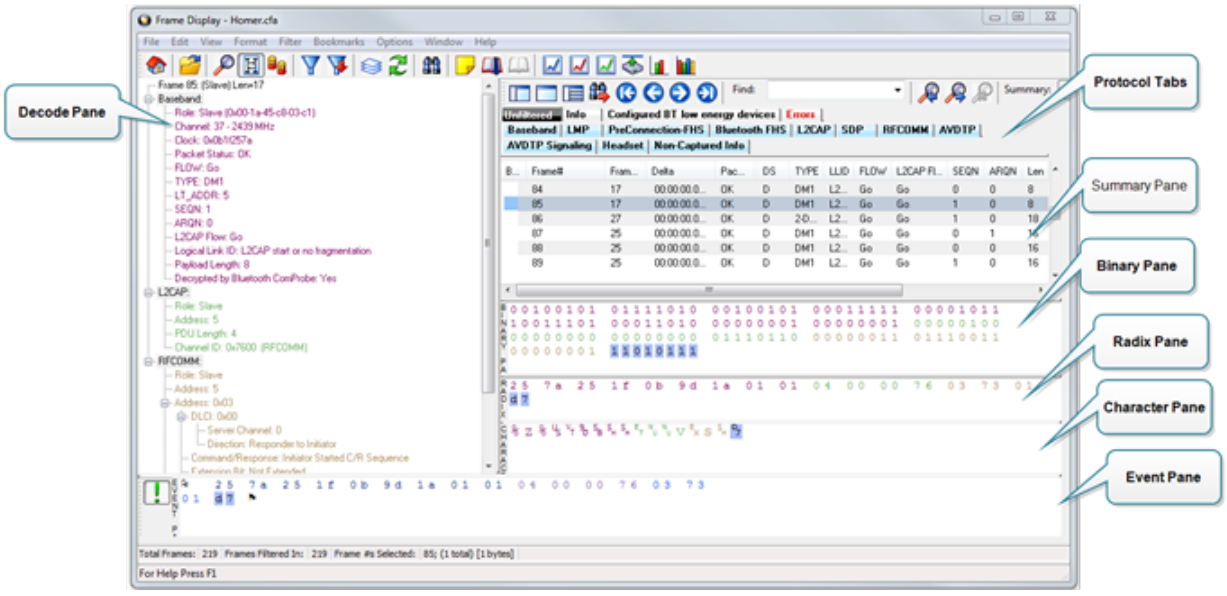


Figure 4.12 - Frame Display with all panes active

Frame Display Panes

The **Frame Display** window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame.

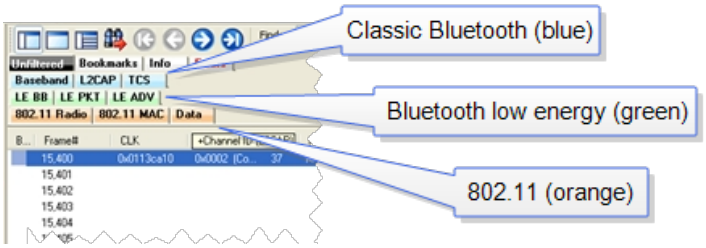
- Summary Pane - The **Summary Pane** displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.
- Decode Pane - The **Decode Pane** displays a detailed decode of the highlighted frame. Fields selected in the **Decode Pane** have the appropriate bit(s) or byte(s) selected in the **Radix**, **Binary**, **Character** , and **Event** panes
- Radix Pane - The **Radix Pane** displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.
- Binary Pane - The **Binary Pane** displays a binary representation of the logical data bytes.
- Character Pane - The **Character Pane** displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.
- Event Pane - The Event Pane displays the physical data bytes in the frame, as received on the network.

By default, all panes except the **Event Pane** are displayed when the Frame Display is first opened.

Protocol Tabs

Protocol filter tabs are displayed in the **Frame Display** above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth (blue), Bluetooth low energy (green), 802.11 (orange), USB (purple), NFC (brown) and SD (teal). The General group applies to all technologies. The other groups are technology-specific.



- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet's technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.
- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic Bluetooth and Bluetooth low energy , there will be L2CAP tabs in the General group, the Classic Bluetooth group, and the Bluetooth low energy group.

Select the **Unfiltered** tab to display all packets.

There are several special tabs that appear in the **Summary Pane** when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

Comparing Frames

If you need to compare frames, you can open additional **Frame Display** windows by clicking on the **Duplicate View** icon . You can have as many **Frame Display** windows open at a time as you wish.

Frame Wrapping and Display

In order to assure that the data you are seeing in **Frame Display** are current, the following messages appear describing the state of the data as it is being captured.

- All **Frame Display** panes except the Summary pane display "No frame selected" when the selected frame is in the buffer (i.e. not wrapped out) but not accessible in the **Summary** pane. This can happen when a tab is selected that doesn't filter in the selected frame.
- When the selected frame wraps out (regardless of whether it was accessible in the Summary pane) all **Frame Display** panes except the **Summary** pane display "Frame wrapped out of buffer".

- When the selected frame is still being captured, all **Frame Display** panes except the Summary pane display "Frame incomplete".

4.4.1.1 Frame Display Toolbar

The buttons that appear in the **Frame Display** window vary according to the particular configuration of the analyzer. For controls not available the icons will be grayed-out.

Table 4.5 - Frame Display Toolbar Icons

Icon	Description
	Control – Brings the Control window to the front.
	Open File - Opens a capture file.
	I/O Settings - Opens the I/O Settings dialog.
	Start Capture - Begins data capture to a user designated file.
	Stop Capture - Closes a capture file and stops data capture to disk.
	Save - Save the currently selected bytes or the entire buffer to file.
	Clear- Discards the temporary file and clears the display.
	Event Display – Brings the Event Display window to the front.
	Show Message Sequence Chart - Message Sequence Chart (MSC) displays information about the messages passed between protocol layers.
	Duplicate View - Creates a second Frame Display window identical to the first.
	Apply/Modify Display Filters - Opens the Display Filter dialog.
	Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.
	Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data

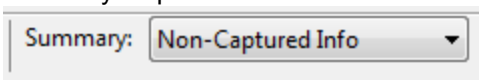
Table 4.5 - Frame Display Toolbar Icons(continued)

Icon	Description
	Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.
	Find - Search for errors, string patterns, special events and more.
	Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.
	Add/Modify Bookmark - Add a new or modify an existing bookmark.
	Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.
	Bluetooth Timeline - Opens the Bluetooth Timeline
	Coexistence View - Opens the Coexistence View
	low energy Timeline- Opens the low energy Timeline
	Extract Data - Opens the Extract Data dialog.
	Bluetooth low energy Packet Error Rate Statistics Opens the Packet Error Rate Statistics display
	Bluetooth Classic Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.
Reload Decoders - When **Reload Decoders** is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.	

Table 4.5 - Frame Display Toolbar Icons(continued)

Icon	Description
Filter:	Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.
The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.	
	Show Default Panes - Returns the panes to their default settings.
	Show Only Summary Pane - Displays only the Summary pane.
	Shall All Panes Except Event Pane - Makes the Decode pane taller and the Summary pane narrower.
	Toggle Display Lock - Prevents the display from updating.
	Go To Frame
	First Frame - Moves to the first frame in the buffer.
	Previous Frame - Moves to the previous frame in the buffer.
	Next Frame - Moves to the next frame in the buffer.
	Last Frame - Moves to the last frame in the buffer.
Find:	Find on Frame Display only searches the Decode Pane for a value you enter in the text box.
	Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.
	Find Next Occurrence - Moves to the next occurrence of the value in the Frame Display Find.

Table 4.5 - Frame Display Toolbar Icons(continued)

Icon	Description
	Cancel Current Search - Stops the current Frame Display Find.
Summary:	Summary Drop Down Box: Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a low energy predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled. 
Text with Protocol Stack: To the right of the Summary Layer box is some text giving the protocol stack currently in use.	

Note: If the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

4.4.1.2 Frame Display Status Bar

The **Frame Display Status** bar appears at the bottom of the **Frame Display**. It contains the following information:

- **Frame #s Selected**: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses
- **Total Frames**: The total number of frames in the capture buffer or capture file in real-time
- **Frames Filtered In**: The total number of frames displayed in the filtered results from user applied filters in real-time

4.4.1.3 Hiding and Revealing Protocol Layers in the Frame Display

Hiding protocol layers refers to the ability to prevent a layer from being displayed on the **Decode** pane. Hidden layers remain hidden for every frame where the layer is present, and can be revealed again at any time. You can hide as many layers as you wish.

Note: Hiding from the **Frame Display** affects only the data shown in the **Frame Display** and not any information in any other window.

There are two ways to hide a layer.

1. Right-click on the layer in the **Decode** pane, and choose **Hide** [protocol name] **Layer In All Frames**.
2. Click the **Set Protocol Filtering** button on the **Summary** pane toolbar. In the **Protocols to Hide** box on the right, check the protocol layer(s) you want hidden. Click **OK** when finished.

To reveal a hidden protocol layer:

1. Right-click anywhere in the **Decode** pane
2. Choose **Show** [protocol name] **Layer** from the right-click menu, or click the S**et Protocol Filtering** button and un-check the layer or layers you want revealed.

4.4.1.4 Physical vs. Logical Byte Display

The **Event Display** window and **Event Pane** in the **Frame Display** window show the physical bytes. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the logical data, or the resulting byte values after escape codes or other character altering codes have been applied (a process called transformation).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane displays 0x7d 0x23, while the Radix pane displays 0x03.

4.4.1.5 Sorting Frames

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the **Summary** pane to sort the frames by that column. For example, to sort the frames by size, click on the **Frame Size** column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

4.4.1.6 Frame Display - Find

Frame Display has a simple **Find** function that you can use to search the Decode Pane for any alpha numeric value. This functionality is in addition to the more robust Search/Find dialog.

Frame Display Find is located below the toolbar on the **Frame Display** dialog.

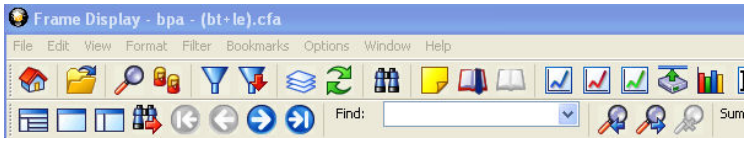


Figure 4.13 - Frame Display Find text entry field

Where the more powerful Search/Find functionality searches the **Decode**, **Binary**, **Radix**, and **Character** panes on **Frame Display** using TImestamps, Special Events, Bookmarks, Patterns, etc.,

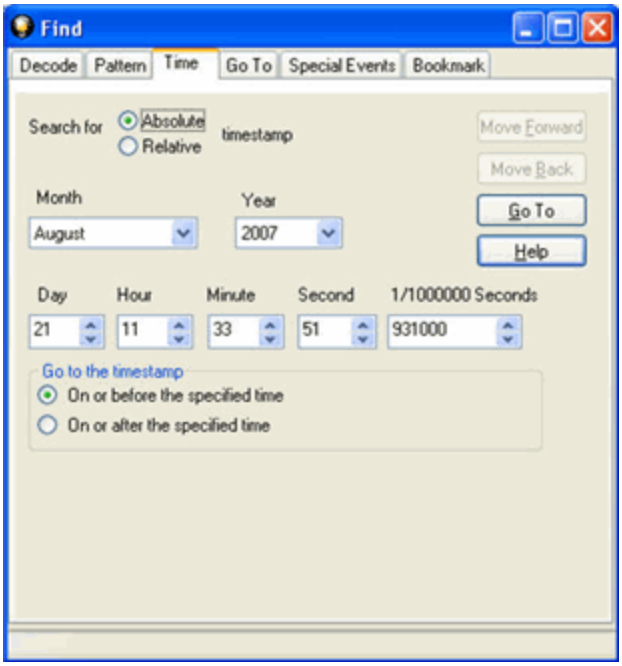


Figure 4.14 - Search/Find Dialog

Find on **Frame Display** only searches the Decode Pane for a value you enter in the text box.

To use **Find**:

1. Select the frame where you want to begin the search.

2. Enter a value in the **Find** text box.

Note: Note: The text box is disabled during a live capture.

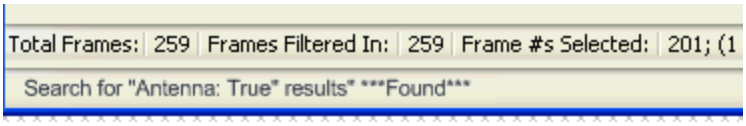
Select **Find Previous Occurrence** to begin the search on frames prior to the frame you selected, or **Find Next Occurrence** to begin the search on frames following the frame you selected.

The next occurrence of the value (if it is found) will be highlighted in the Decode Pane.

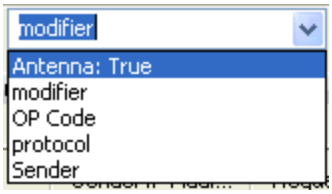
4. Select **Find Previous Occurrence** or **Find Next Occurrence** to continue the search.

There are several important concepts to remember with Find.

- When you enter a search string and select Enter, the search moves forward.
- If you select **Find Previous Occurrence**, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous Occurrence.
- If you select **Find Next Occurrence**, when the search reaches the last frame it will then cycle to the first frame and continue until it reaches the frame where the search began.
- F3 is a shortcut for Find Next Occurrence.
- You cannot search while data is being captured.
- After a capture is completed, you cannot search until Frame Display has finished decoding the frames.
- Find is not case sensitive.
- The status of the search is displayed at the bottom of the dialog.
- The search occurs only on the protocol layer selected.
- To search across all the protocols on the Frame Display, select the Unfiltered tab.



- A drop-down list displays the search values entered during the current session of Frame Display.
- The search is cancelled when you select a different protocol tab during a search.
- You can cancel the search at any time by selecting the **Cancel Current Search** button.



4.4.1.7 Synchronizing the Event and Frame Displays

The **Frame Display** is synchronized with the **Event Display.** Click on a frame in the **Frame Display** and the corresponding bytes is highlighted in the **Event Display**. Each **Frame Display** has its own **Event Display**.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the **Frame Display** icon in **Control** window toolbar to open the **Frame Display.**
2. Click on the **Duplicate View** icon to create **Frame Display** #2.
3. Click on **Event Display** icon in **Frame Display** #2. **Event Display** #2 opens. This **Event Display** is labeled #2, even though there is no original **Event Display**, to indicate that it is synchronized with **Frame Display** #2.
4. Click on a frame in **Frame Display** #2. The corresponding bytes are highlighted in **Event Display** #2.
5. Click on a frame in the original **Frame Display**. **Event Display** #2 does not change.

4.4.1.8 Working with Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the **Duplicate View** icon on the **Frame Display** toolbar.

  This creates another **Frame Display** window. You can have as many **Frame Displays** open as you wish. Each **Frame Display** is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the **Frame Display** icon in the Control window toolbar.

  A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one **Frame Display**, that filter does not automatically appear in the other **Frame Display**. You must use the Hide/Reveal feature to display a filter created in one Frame Display in another.

Note: When you have multiple **Frame Display** windows open and you are capturing data, you may receive an error message declaring that "Filtering cannot be done while receiving data this fast." If this occurs, you may have to stop filtering until the data is captured.

4.4.1.9 Working with Panes on Frame Display

When the **Frame Display** first opens, all panes are displayed except the **Event** pane (To view all the panes, select **Show All Panes** from the **View** menu).

- The **Toggle Expand Decode Pane** icon makes the decode pane longer to view lengthy decodes better.
- The **Show Default Panes** icon returns the **Frame Display** to its default settings.
- The Show only Summary Pane icon displays on the Summary Pane.

To close a pane, right-click on the pane and select **Hide This Pane** from the pop-up menu, or de-select **Show [Pane Name]** from the **View** menu.

To open a pane, right-click on the any pane and select **Show Hidden Panes** from the pop-up menu and select the pane from the fly-out menu, or select **Show [Pane Name]** from the **View** menu.

To re-size a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to re-size the pane.

4.4.1.10 Frame Display - Byte Export

The captured frames can be exported as raw bytes to a text file.

1. From the **Frame Display File** menu select **Byte Export...**.

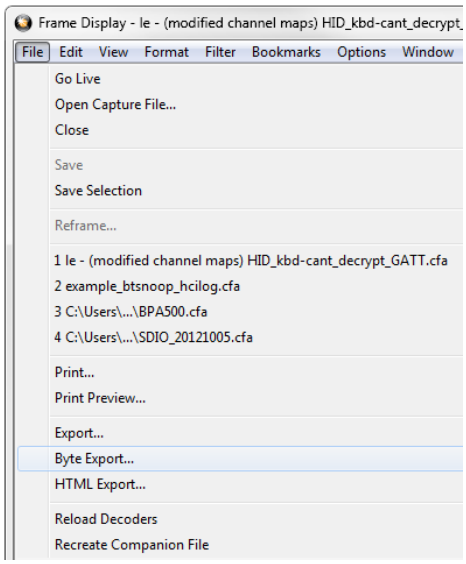


Figure 4.15 - Frame Display File menu, Byte Export

2. From the Byte Export window specify the frames to export.

   - All Frames exports all filtered-in frames including those scrolled off the **Summary** pane. Filtered-in frames are dependent on the selected **Filter** tab above the **Summary** pane. Filtered-out frames are not exported.
   - Selected Frames export is the same as **All Frames** export except that only frames selected in the **Summary** pane will be exported.

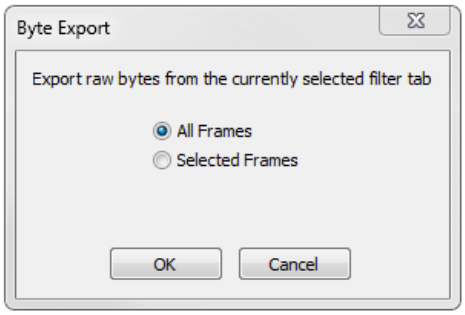


Figure 4.16 - Byte Export dialog

   Click the **OK** button to save the export. Clicking the **Cancel** button will exit Byte Export.

3. The **Save As** dialog will open. Select a directory location and enter a file name for the exported frames file.

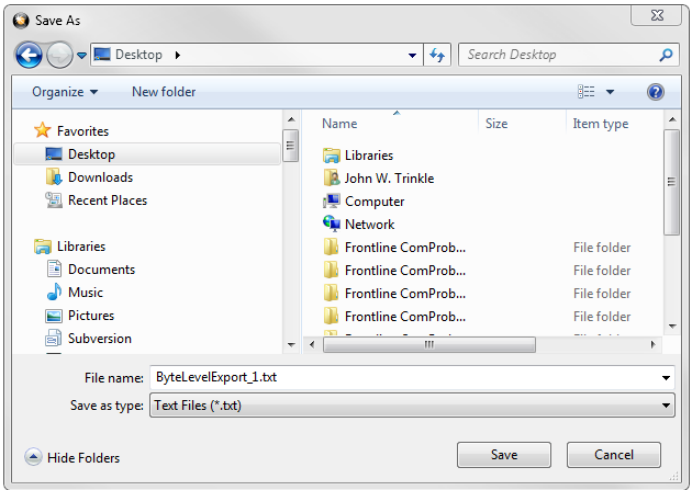


Figure 4.17 - Save As dialog

Click on the **Save** button.

The exported frames are in a text file that can be opened in any standard text editing application. The header shows the export type, the capture file name, the selected filter tab, and the number of frames. The body shows the frame number, the timestamp in the same format shown in the **Frame Display Summary** pane, and the frame contents as raw bytes.

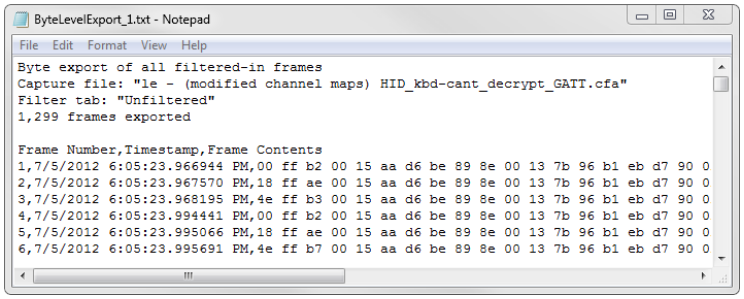

ByteLevelExport_1.txt - Notepad
File Edit Format View Help
Byte export of all filtered-in frames
Capture file: "le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa"
Filter tab: "Unfiltered"
1,299 frames exported
Frame Number,Timestamp,Frame Contents
1,7/5/2012 6:05:23.966944 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
2,7/5/2012 6:05:23.967570 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
3,7/5/2012 6:05:23.968195 PM,4e ff b3 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
4,7/5/2012 6:05:23.994441 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
5,7/5/2012 6:05:23.995066 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
6,7/5/2012 6:05:23.995691 PM,4e ff b7 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0

Figure 4.18 - Sample Exported Frames Text File

4.4.1.11 Panes in the Frame Display

4.4.1.11.1 Summary Pane

The **Summary** pane displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

The ComProbe USB **Summary** pane in displays a one-line summary of every transaction in a capture buffer or

file. Whenever there is a transaction it is shown on a single line instead of showing the separate messages that comprise the transaction. The **Msg** column in that case says "Transaction".

Each message in a transaction contains a packet identifier (PID). All of the PIDs in a transaction are shown in the transaction line.

All "IN" transactions (i.e. transactions that contain an IN token message) are shown with a purple background. All other transactions and all non-transactions are shown with a white background. "IN" transactions have special coloring because that is the only place where the primary data flow is from a device to the Host.

The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred is displayed in red. The Decode Pane gives precise information as to the type of error and where it occurred.

The **Summary** pane is synchronized with the other panes in this window. Click on a frame in the **Summary** pane, and the bytes for that frame is highlighted in the **Event** pane while the **Decode** pane displays the full decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

Protocol Tabs

Protocol filter tabs are displayed in the Frame Display above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth® (blue), *Bluetooth* low energy (green), 802.11 (orange), USB (purple), and SD (brown). The General group applies to all technologies. The other groups are technology-specific.

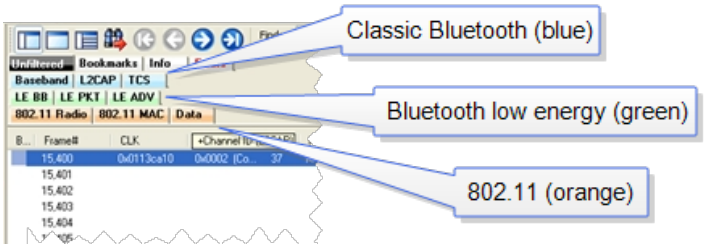


Figure 4.19 - Example Protocol Tags

- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet's technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.
- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic *Bluetooth* and *Bluetooth* low energy , there will be L2CAP tabs in the General group, the Classic *Bluetooth* group, and the *Bluetooth* low energy group.

Select the Unfiltered tab to display all packets.

There are several special tabs that appear in the **Summary** pane when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

Use the navigation icons, keyboard or mouse to move through the frames. The icons and move you to the first and last frames in the buffer, respectively. Use the Go To icon to move to a specific frame number.

Placing the mouse pointer on a summary pane header with truncated text displays a tooltip showing the full header text.

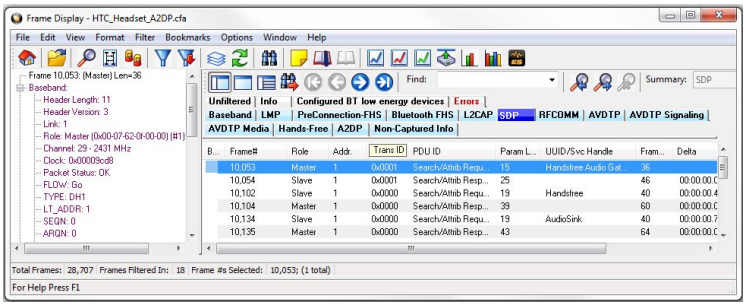

Frame Display - HTC_Headset_A2DP.cfa
File Edit View Format Filter Bookmarks Options Window Help
Unfiltered | Info | Configured BT low energy devices | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVDTP | AVDTP Signaling
AVDTP Media | Hands-Free | A2DP | Non-Captured Info
Trans ID
PDU ID
Total Frames: 28,707 Frames Filtered In: 18 Frame #s Selected: 10,053; (1 total)
For Help Press F1

Figure 4.20 - Summary pane (right) with Tooltip on Column 5 (Tran ID)

Sides in *Bluetooth* low energy

A Bluetooth low energy data connection consists of connection events, which are a series of transmissions on the same channel. In each connection event the master transmits first, then the slave, and then the devices take turns until the connection event is finished.

When the data connection is encrypted and the packets are successfully decrypted, the sniffer can determine exactly who sent which packet (only non-empty, encrypted packets – empty packets are never encrypted). These packets are labeled either 'M' for master or 'S' for slave.

When the data connection is unencrypted or when encrypted packets are not successfully decrypted by the sniffer, the sniffer cannot distinguish the two devices' (master and slave) packets by their content, just by the packet timing. In those cases we label each device as side '1' or '2', not as master or slave. In each connection event, packets sent by the device which transmitted first in the connection event are labeled '1', and packets sent by the device which transmitted second are labeled '2'.

If no packets in the connection event are missed by the sniffer, the device labeled '1' is the master and the device labeled '2' is the slave. However, if we do not capture the very first packet in a connection event (i.e. the packet sent by the master) but do capture the packet sent by the slave, we label the slave as side '1' since it is the first device we heard in the connection event. Because there is potential clock drift since the last connection event,

we cannot use the absolute timing to correct this error; there would still be cases where we get it wrong. Therefore we always assign '1' to the first packet in a connection event. So even though it is rare, there are connection events where packets sent by the slave device are labeled '1' and packets sent by the master are labeled '2'.

Finally, in a noisy environment it is also possible that the sniffer does not capture packets in the middle of a connection event. If this occurs and the sniffer cannot determine the side for the remaining packets in that connection event, the side is labeled 'U' for "unknown".

4.4.1.11.2 Customizing Fields in the Summary Pane

You can modify the **Summary** Pane in **Frame Display**.

Summary pane columns can be reordered by dragging any column to a different position.

Fields from the **Decode** pane can be added to the summary pane by dragging any **Decode**pane field to the desired location in the **summary** pane header. If the new field is from a different layer than the summary pane a plus sign (+) is prepended to the field name and the layer name is added in parentheses. The same field can be added more than once if desired, thus making it possible to put the same field at the front and back (for example) of a long header line so that the field is visible regardless of where the header is scrolled to.

An added field can be removed from the **Summary** pane by selecting **Remove New Column** from the right-click menu.

The default column layout (both membership and order) can be restored by selecting **Restore Default Columns** from the **Format** or right-click menus.

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The **Frame Size**, **Timestamp**, and **Delta** columns can be hidden by right-clicking on the header and selecting **Show Frame Size Column, Show Timestamp Column,** or **Show Delta Column**. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose **Restore Default Column Widths**, or select **Restore Default Column Widths** from the **Format** menu.

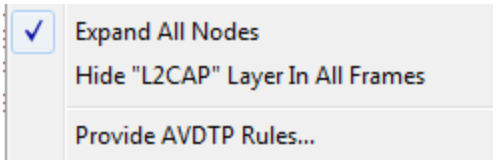
4.4.1.11.3 Frame Symbols in the Summary Pane

Table 4.6 - Frame Symbols

Symbol	Description
	A green dot means the frame was decoded successfully, and the protocol listed in the **Summary Layer** drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the **Summary Layer** drop-down box does not exist in the frame.
	A green circle means the frame was not fully decoded. There are several reasons why this might happen. • One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot. • Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has changed. If the analyzer does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.
	A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

4.4.1.11.4 Decode Pane

The **Decode** pane (aka detail pane) is a post-process display that provides a detailed decode of each frame transaction (sometimes referred to as a frame). The decode is presented in a layered format that can be expanded and collapsed depending on which layer or layers you are most interested in. Click on the plus sign to expand a layer. The plus sign changes to a minus sign. Click on the minus sign to collapse a layer. **Select Show All** or **Show Layers** from the **Format** menu to expand or collapse all the layers. Layers retain their expanded or collapsed state between frames.



Protocol layers can be hidden, preventing them from being displayed on the **Decode** pane. Right-click on any protocol layer and choose **Hide** [protocol name] from the right-click menu.

In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is

applied to layers when the detail pane displays a single message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction between layers and messages clear, each header of each message in the detail pane ends with the word “Message” or “Messages”. The latter is used because data and handshake messages are shown as a single color-coded entry

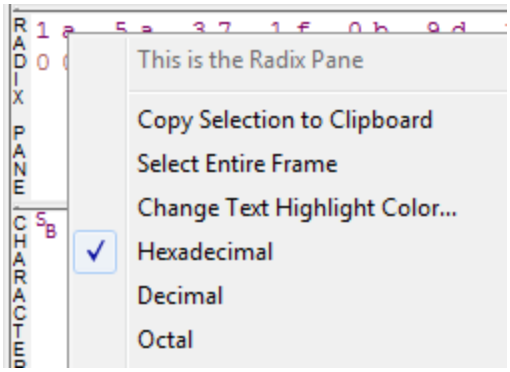
Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the **Event**, **Radix**, **Binary** and **Character** panes. The colors are not assigned to a protocol, but are assigned to the layer.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

Click the **Toggle Expand Decode Pane** icon to make the **Decode** pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

4.4.1.11.5 Radix or Hexadecimal Pane

The **Radix** pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the **Format** menu, or by right-clicking on the pane and choosing **Hexadecimal**, **Decimal** or **Octal**.



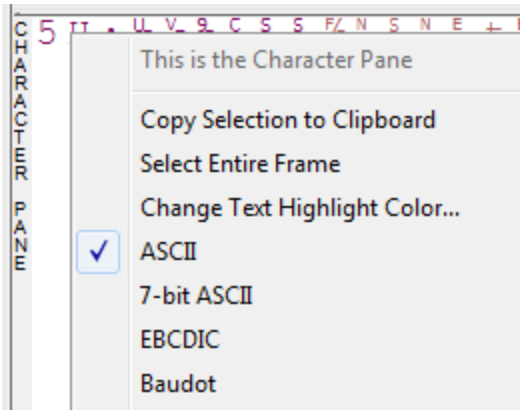
Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.6 Character Pane

The **Character** pane represents the logical bytes in the frame in **ASCII**, **EBCDIC** or **Baudot**. The character set can be changed from the **Format** menu, or by right-clicking on the pane and choosing the appropriate character set.



Because the **Character** pane displays the logical bytes rather than the physical bytes, the data in the **Character** pane may be different from that in the **Event** pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.7 Binary Pane

The **Binary** pane displays the logical bytes in the frame in binary.

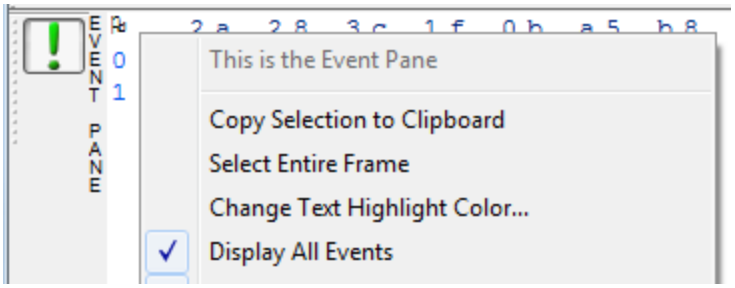
Because the **Binary** pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the **Event** pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.8 Event Pane

The **Event** pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the **All Events** icon .



Displaying all events means that special events, such as **Start of Frame**, **End of Frame** and any signal change events, are displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the **Event Display** window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

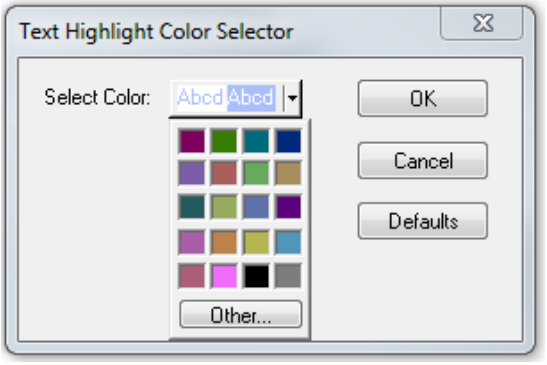
Because the **Event** pane displays the physical bytes rather than the logical bytes, the data in the **Event** pane may be different from that in the **Radix**, **Binary** and **Character** panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.9 Change Text Highlight Color

Whenever you select text in the **Binary**, **Radix**, or **Character** panes in **Frame Display**, the text is displayed with a highlight color. You can change the color of the highlight.



1. Select **Change Text Highlight Color** from the **Options** menu. You can also access the option by right clicking in any of the panes.
2. Select a color from the drop-down menu.
3. Click **OK**.

The highlight color for the text is changed.

Select **Cancel** to discard any selection. Select **Defaults** to return the highlight color to blue.

4.4.1.12 Protocol Layer Colors

4.4.1.12.1 Data Byte Color Notation

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the **Decode** pane is in the same color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the **Summary** pane, frame numbers in red mean there is an error in the frame. Also, the **Errors** tab is displayed in red. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the **Radix**, **Character**, **Binary** and **Event** panes mean there is a physical error associated with the byte.

4.4.1.12.2 Changing Protocol Layer Colors

You can differentiate different protocol layers in the **Decode**, **Event**, **Radix**, **Binary** and **Character** panes.

1. Choose **Select Protocol Layer Colors** from the **Options** menu to change the colors used.

   The colors for the different layers is displayed.

2. To change a color, click on the arrow next to each layer and select a new color.

3. Select **OK** to accept the color change and return to **Frame** Display.

Select **Cancel** to discard any selection. Select **Defaults** to return the highlight colors to the default settings.

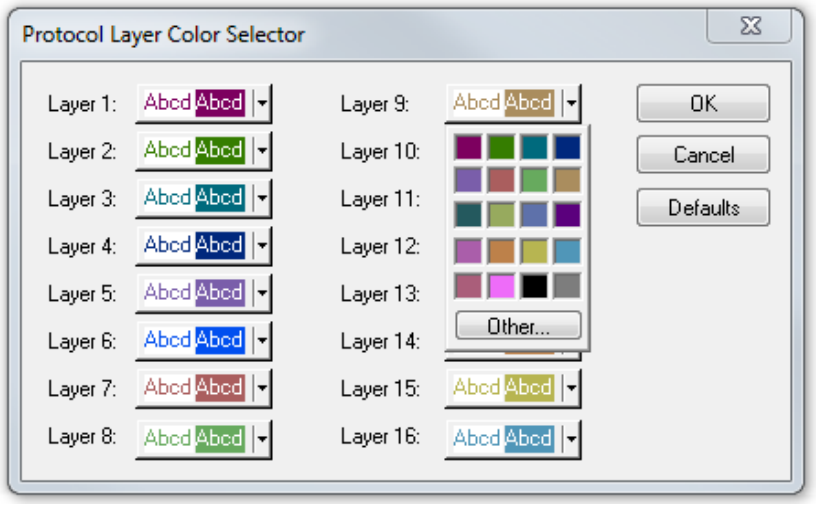


Figure 4.21 - Frame Display Protocol Layer Color Selector

4.4.1.13 Filtering

Filtering allows the user to control the display which capture frames are displayed. Filters fall into two general categories:

1. **Display filters** allow a user to look at a subset of captured data without affecting the capture content. Frames matching the filter criteria appear in the **Frame Display**; frames not matching the criteria will not appear.
2. **Connection filters** Two options are available.
    a. A Bluetooth connection: Displays only the frames associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address. A new **Frame Display** will open showing only the protocol tabs, frames, summary, and events associated with that particular *Bluetooth* connection.
    b. A specific wireless or wired technology. Displays all of the frames associated with:
        - Classic *Bluetooth*
        - *Bluetooth* low energy
        - 802.11
        - HCI

        A new Frame Display will open showing only the protocol tabs, frames, summary and events associated with the selected technology.

4.4.1.13.1 Display Filters

A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filter

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.

- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog.

4.4.1.13.1.1 Creating a Display Filter

There are two steps to using a display filter. Define the filter conditions, and then apply the filter to the data set. The system combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters** from the **Filter** menu to open the **Set Condition** dialog box. The Set Condition dialog is self configuring which means that when you **Select each frame** under **Conditions** the following displayed fields depend on your selection. With each subsequent selection the dialog fields will change depending on you selection in that field.

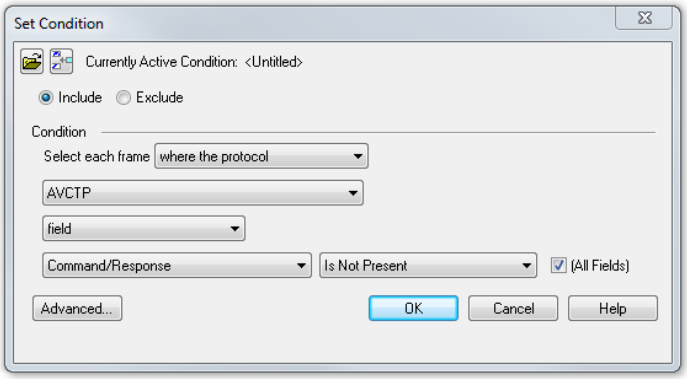


Figure 4.22 - Example: Set Conditions Self Configuring Based on Protocol Selection

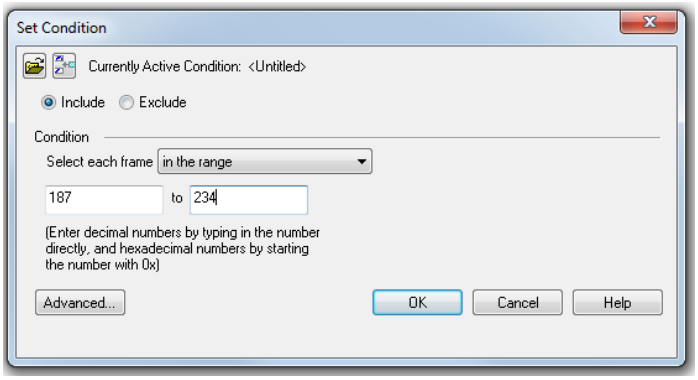


Figure 4.23 - Example: Set Conditions Self Configuring Based on Frame Range

2. Select **Include** or **Exclude** to add filtered data or keep out filtered data respectively.
3. Select the initial condition for the filter from the drop-down list.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.
5. Click OK. The system displays the **Save Named Condition** dialog. Provide a name for the filter condition or accept the default name provided by the system and click **OK**. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The **Set Condition** dialog box closes, creates a tab on the **Frame Display** with the filter name, and applies the filter.

The filter also appears in the Quick Filtering and Hiding Protocols dialog.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Notes:

- The system requires naming and saving of all filters created by the user.
- The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.
- When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other **Frame Display** windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different **Frame Display** window.

4.4.1.13.1.2 Including and Excluding Radio Buttons

All filter dialog boxes contain an **Include** and an **Exclude** radio button. These buttons are mutually exclusive. The **Include/Exclude** selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

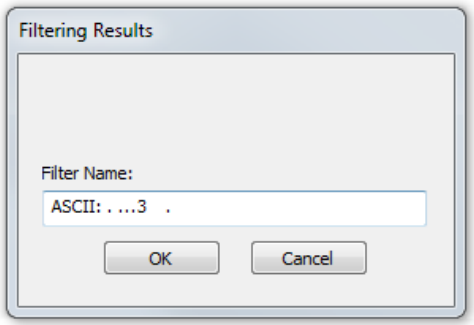
Include: A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

Exclude: A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

4.4.1.13.1.3 Named Display Filters

You can create a unique display filter by selecting a data type on the **Frame Display** and using a right click menu. When you create a **Name Filter**, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the **Frame Display** panes.

1. Select a frame in the **Frame Display Summary** Pane.
2. Right click in the one of the data columns in the **Summary** Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select **Filter in *(data type)* =** . The **Filtering Results** dialog appears.
4. Enter a name for the filter
5. Select **OK**.



The filter you just created appears in the **Named Filters** section of the Quick Filtering dialog.

4.4.1.13.1.4 Using Compound Display Filters

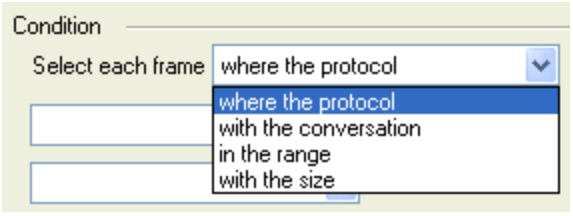
Compound filters use boolean logic to create complex and precise filters. There are three primary Boolean logic operators: **AND**, **OR**, and **NOT**.

The **AND** operator narrows the filter, the **OR** operator broadens the filter, and the **NOT** operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the filter menu to open the **Set Condition** dialog box.
2. Click the **Advanced** button on the **Set Condition** dialog box.
3. Select **Include** or **Exclude** radio button.

   Now you can set the conditions for the filter.
4. Select the initial condition for the filter from the combo box at the bottom of the dialog for **Select each frame.**
5. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.



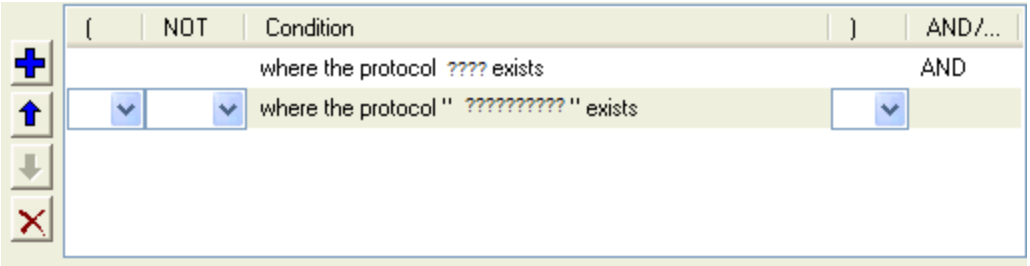


Figure 4.24 - Two Filter Conditions Added with an AND Operator

6. Click the plus icon on the left side of the dialog box and repeat steps 4 and 5 for the next condition. Use the up and down arrow icons on the left side of the dialog box to order your conditions, and the delete button to delete conditions from your filter.
7. Continue adding conditions until your filter is complete.
8. Include parentheses as needed and set the boolean operators.
9. Click **OK**.
10. The system displays the **Save Named Condition** dialog. Provide a name for the filter condition or accept the default name provided by the system and click **OK**.

Figure 4.25 - Save Named Filter Condition Dialog

The **Set Condition** dialog box closes, creates a tab on the **Frame Display** with the filter name, and applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

4.4.1.13.1.5 Defining Node and Conversation Filters

There are two steps to using Node and Conversation display filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the filter menu to open the **Set Condition** dialog box.
2. From the **Select each frame** combo box choose **frames with the conversation** as the initial condition.
3. Select an address type—IP, MAC, TCP/UDB—from the **Type**combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first **Address** combo box.
5. Choose a direction arrow from the direction box . The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.

6. If you want to filter on just one node address, skip step 7 and continue with step 8.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select a node address from the second Address combo box..
8. Click **OK**. The **Set Condition** dialog box closes and the analyzer applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button is unavailable (grayed out) until the condition selections are complete.

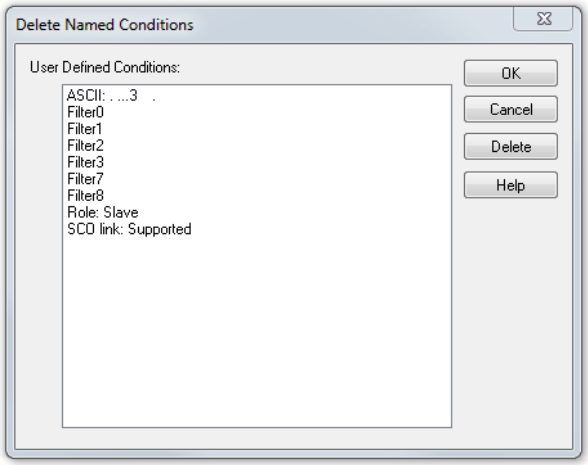
4.4.1.13.1.6 The Difference Between Deleting and Hiding Display Filters

If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the **Set Conditions** dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

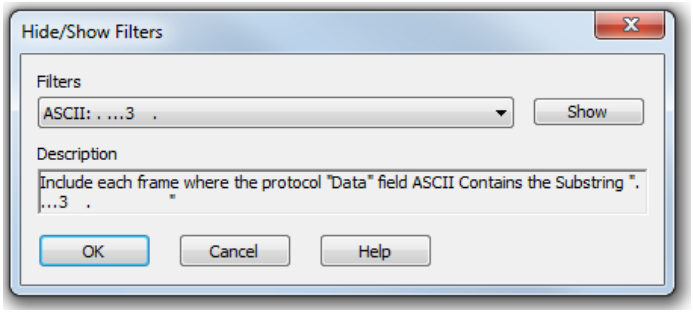
Deleting Saved Display Filters



1. Select **Delete Display Filters** from the **Filter** menu in the **Frame Display** window to open the **Delete Named Condition** dialog. The system displays the **Delete Named Condition** dialog with a list of all user defined filters.
2. Select the filter to be deleted from the list.
3. Click the **Delete** button.
4. Click **OK**. The **Delete Named Condition** dialog box closes and the system deletes the filter.

Hiding and Revealing Display Filters

If a display filter is showing the following steps will hide that filter but will not delete it.



1. **Select Hide/Show Display Filters…** from the **Filter** menu on the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the **Hide** button. The **Hide** button is only showing if the selected filter is currently showing in the **Frame Display**.
4. Click **OK**. The **Hide/Show Filters** dialog box closes, and the system hides the filter and removes the filter tab from the Frame Display.

If a display filter is hidden the following steps will reveal that filter in the **Frame Display**.

1. Select **Hide/Show Display Filters…** from the **Filter** menu in the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the **Show** button.
4. Click **OK**. The **Hide/Show Filters** dialog box closes and the system reveals the filter in the **Frame Display**.

You can also open the Quick Filter dialog and check the box next to the hidden filter to show or hide a display filter.

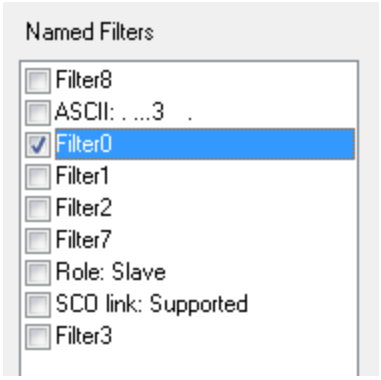


Figure 4.26 - Using Named Filters Section of Quick Filters to Show/Hide Filters

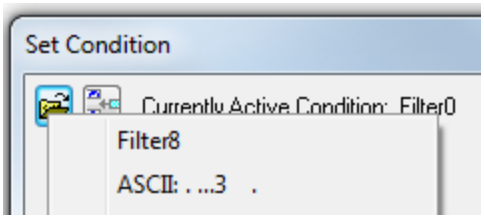
Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Show dialog to display a filter created in one Frame Display in different Frame Display window.

4.4.1.13.1.7 Editing Filters

Modifying a Condition in a Filter

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters...** from the **Filter** menu to open the **Set Condition** dialog box. The **Set Condition** dialog box displays the current filter definition at the top of the dialog.

   To display another filter, click the **Open** icon, and select the filter from the pop-up list of all the saved filters.



2. Edit the desired parameter of the condition: Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click **OK**.) The **Set Condition** dialog box closes, and the system applies the modified filter.

Note: When a display filter is applied, a description of the filter appears to the right of the toolbar in the Frame Display windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

Deleting a Condition in a Filter

If a display filter has two or more conditions you can delete conditions. If there is only one condition set in the filter you must delete the filter using **Delete Display Filters...** from the **Filters** menu.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the **Filter** menu to open the **Set Condition** dialog box. Click on the Advanced button to show the condition in Boolean format. The dialog box displays the current filter definition. To display another filter, click the Open icon, and select the filter from the pop-up list of all the saved filters.

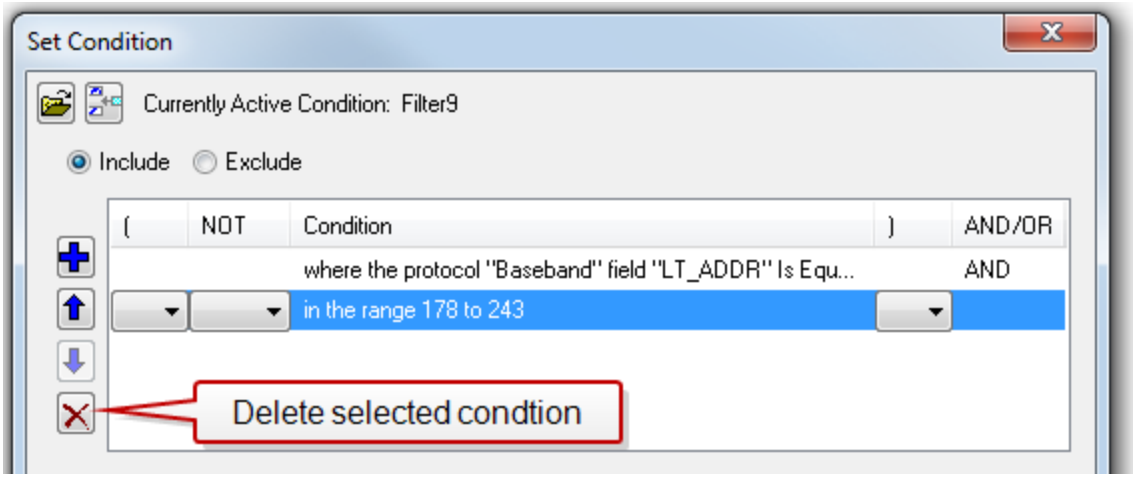


Figure 4.27 - Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.
3. Click the **Delete Selected Line** icon.
4. Edit the Boolean operators and parentheses as needed.
5. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click **OK**.) The **Set Condition** dialog box closes, and the system applies the modified filter.

Note: When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

Renaming a Display Filter

1. Select **Rename Display Filters…** from the **Filter** menu in the **Frame Display** window to open the **Rename Filter** dialog. The system displays the **Rename Filter** dialog with a list of all user defined filters in the **Filters** combo box.

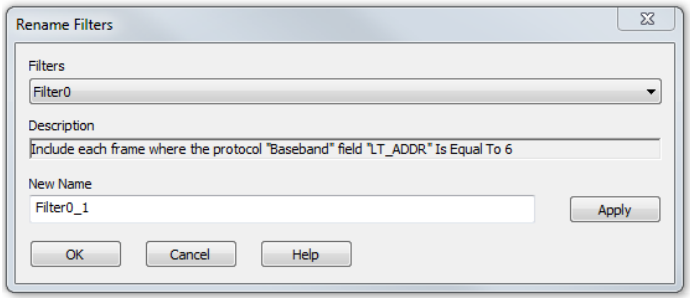


Figure 4.28 - Rename Filters Dialog

2. Select the filter to be renamed from the combo box.
3. Enter a new name for the filter in the **New Name** box. Optionally click the **Apply** button and the new name will appear in the **Filters** combo box and the **New Name** box will empty. This option allows you to rename several filters without closing the **Rename Filter** dialog each time.
4. Click **OK**. The **Rename Filter** dialog box closes and the system renames the filter.

4.4.1.13.2 Connection Filtering

Connection Filtering allows the user to view a subset of the total available packets within the **Frame Display**. The subset can include data from a single *Bluetooth* connection, or all of the BR/EDR packets, all of the low energy packets, all of the 802.11 packets, or all of the HCI packets.

Bluetooth Applicability

A connection (device pair) is identified by

1. A Link for Classic *Bluetooth*,
2. An Access Address for *Bluetooth* low energy.

The link ID is a number that the ComProbe software assigns to identify a pair of devices in a BR/EDR connection. In the **Frame Display** details pane, the Baseband layer contains the link ID field if the field's value is not 0.

An Access Address is contained in every *Bluetooth* low energy packet. The Access Address identifies a connection between a slave and a master or an advertising packet.

Connection filtering displays only the frames, protocols, summary, details, and events for the selected connections.

Note: Connection Filters are not persistent across sessions.

4.4.1.13.2.1 Creating a Connection Filter

In the Frame Display there are four ways to create a connection filter.

From the Frame Display Filter menu

Click on the **Frame Display Filter** menu **Connection Filter** selection. From the drop down menu, select **Classic** or **Bluetooth low energy**. The options are

- Classic *Bluetooth*:
  - **All** will filter in all Classic *Bluetooth* frames. You are in effect filtering out any *Bluetooth* low energy frames and are selecting to filter in all the Classic *Bluetooth* links.
  - **Links** displays all the master-slave links. You can select only one link to filter in. The selected link will filter in only the frames associated with that link.
- *Bluetooth* low energy:
  - **All** will filter in all Bluetooth low energy frames. You are in effect filtering out any Classic Bluetooth frames and are selecting to filter in all Bluetooth low energy access addresses.
  - **Access Addresses** displays all the low energy slave device's access address. You can select only one access address to filter. The selected link will filter in only the frames associated with that access address.
- 802.11:
  - **All** will filter in all 802.11 frames. You are in effect filtering out any other technology frames.
- HCI:
  - **All** will filter in all HCI frames. You are in effect filtering out any other technology frames.

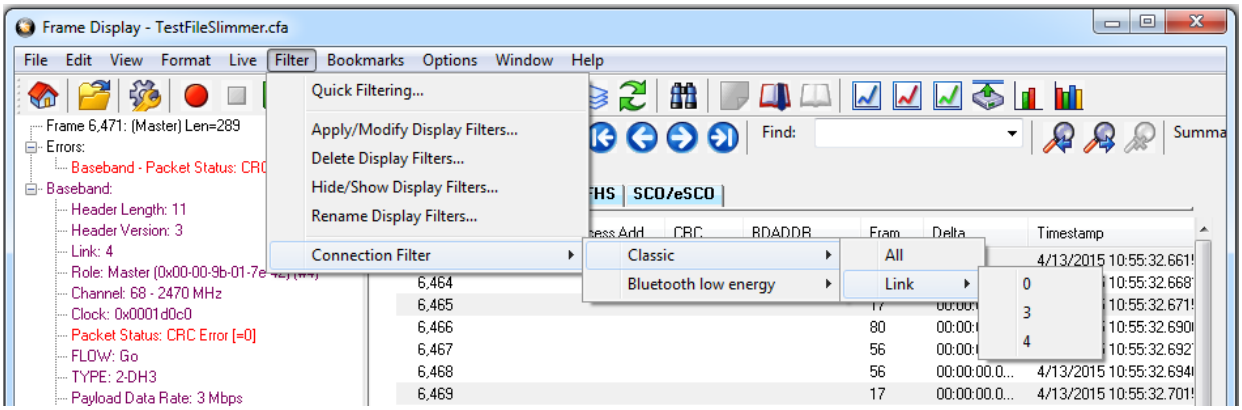


Figure 4.29 - Connection Filter from the Frame Display Menu

From the Frame Display toolbar

Right-click anywhere in the toolbar and select **Connection Filter** from the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

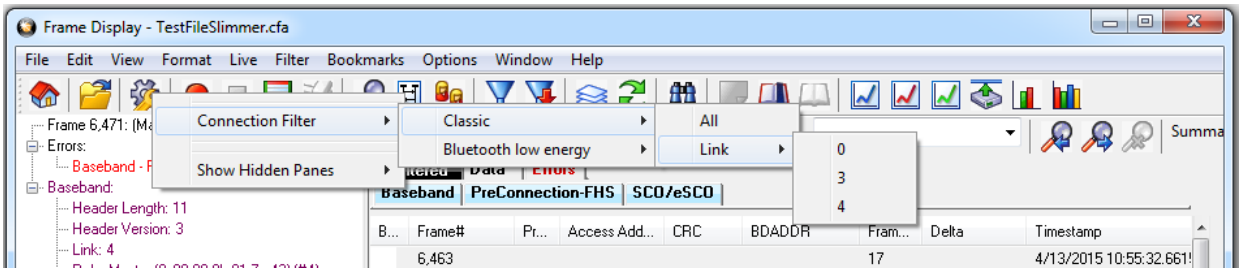


Figure 4.30 - Connection Filter from the Frame Display Toolbar right-click

From the Frame Display panes

Right-click anywhere in a Frame Display pane and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

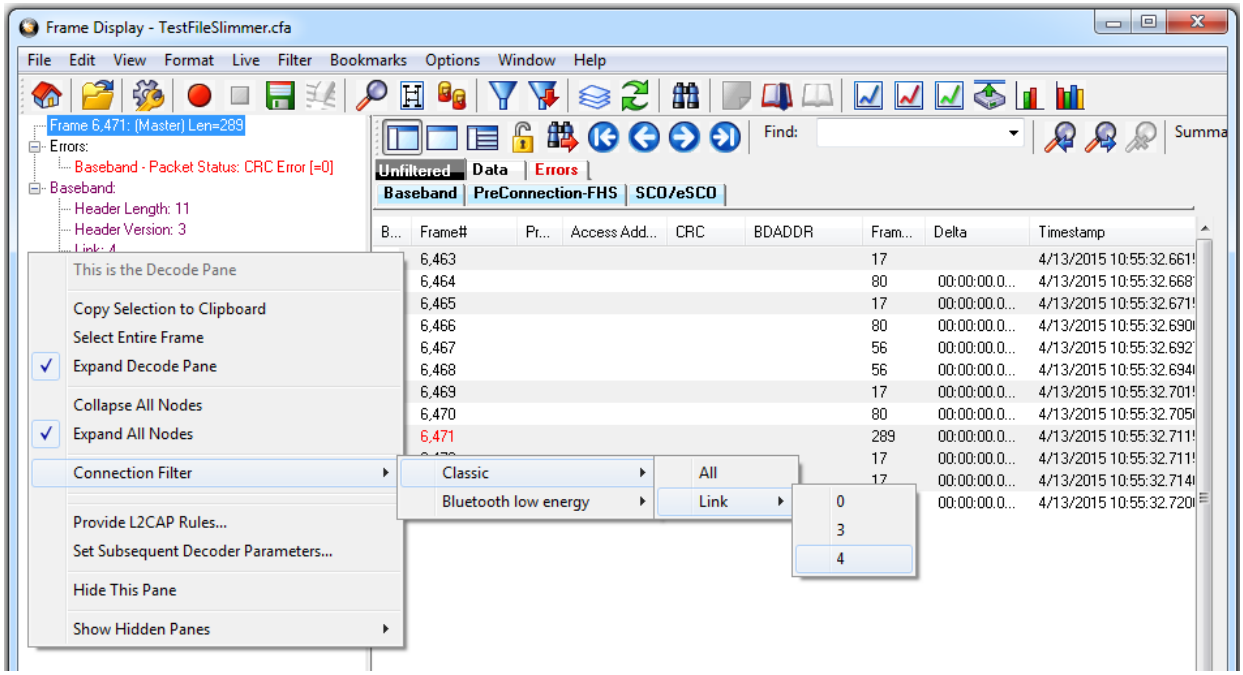


Figure 4.31 - Connection Filter from the Frame Display Pane right-click

From the Frame Display frame selection

Select a frame in the summary pane. Right-click and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

If the frame you have selected is associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address, an additional pop-up menu item will appear as shown in the example image below. This selection is a predetermined filter based on your selection. In the example, frame "6471" is associated with "Link 4", so the predetermined filter assumes that you may want create a connection filter for that link. Clicking on **Connection Filter Link = 4** will filter in "Link 4" frames without opening all the drop-down menus.

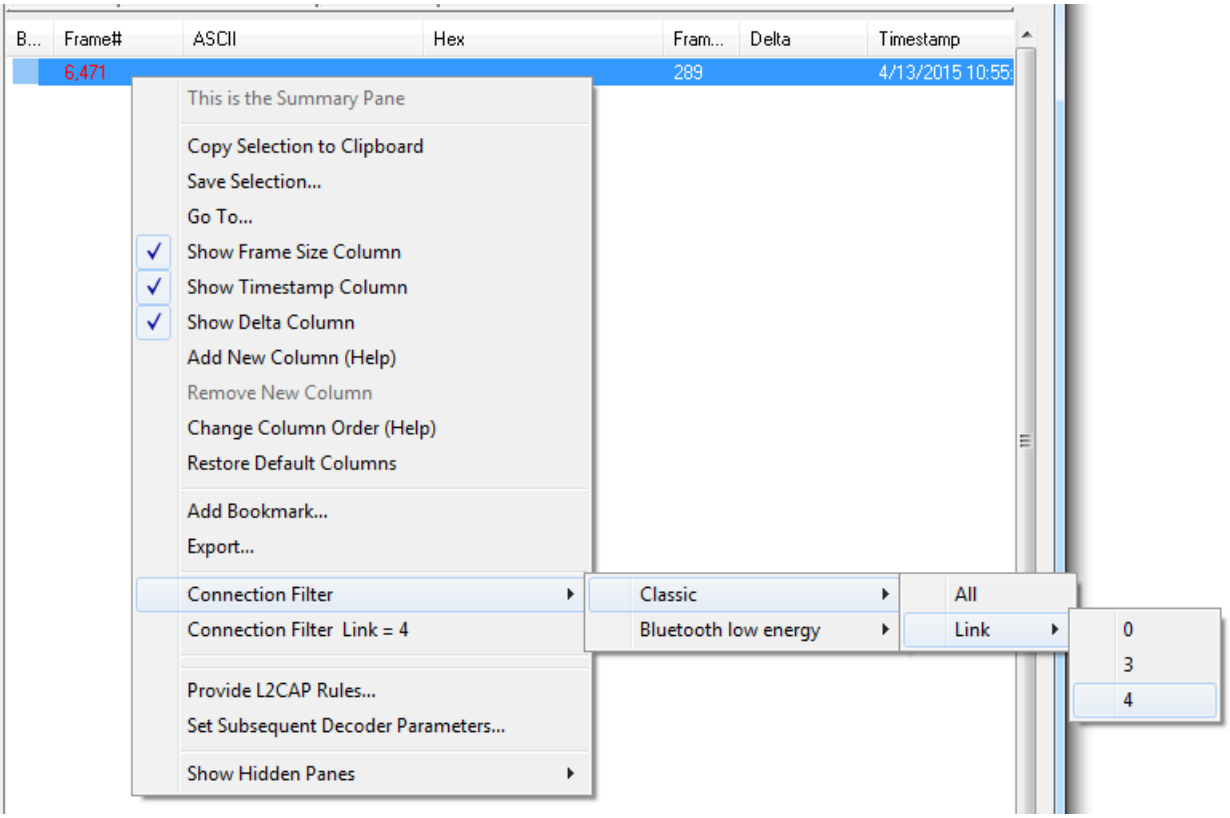


Figure 4.32 - Connection Filter from frame selection right-click

Creating from any Frame Display window

A Connection Filter can be created from any open Frame Display window, and the filtering will always be applied to the original captured data set.

4.4.1.13.2.2 Connection Filter Display

Once you have selected which connections to filter in, another Frame Display will open. The original Frame Display will remain open, and can be minimized.

Note: The system currently limits the number of frame displays to 5. This limit includes any Frame Displays opened using Duplicate View from the Toolbar (see Working with Multiple Frame Displays on page 84)

The new Frame Display with the filtered connection frames will only contain the data defined by the filter criteria. That is, the criteria could be a single link or data for a particular technology.

Display Example 1: Bluetooth low energy Access Address selected

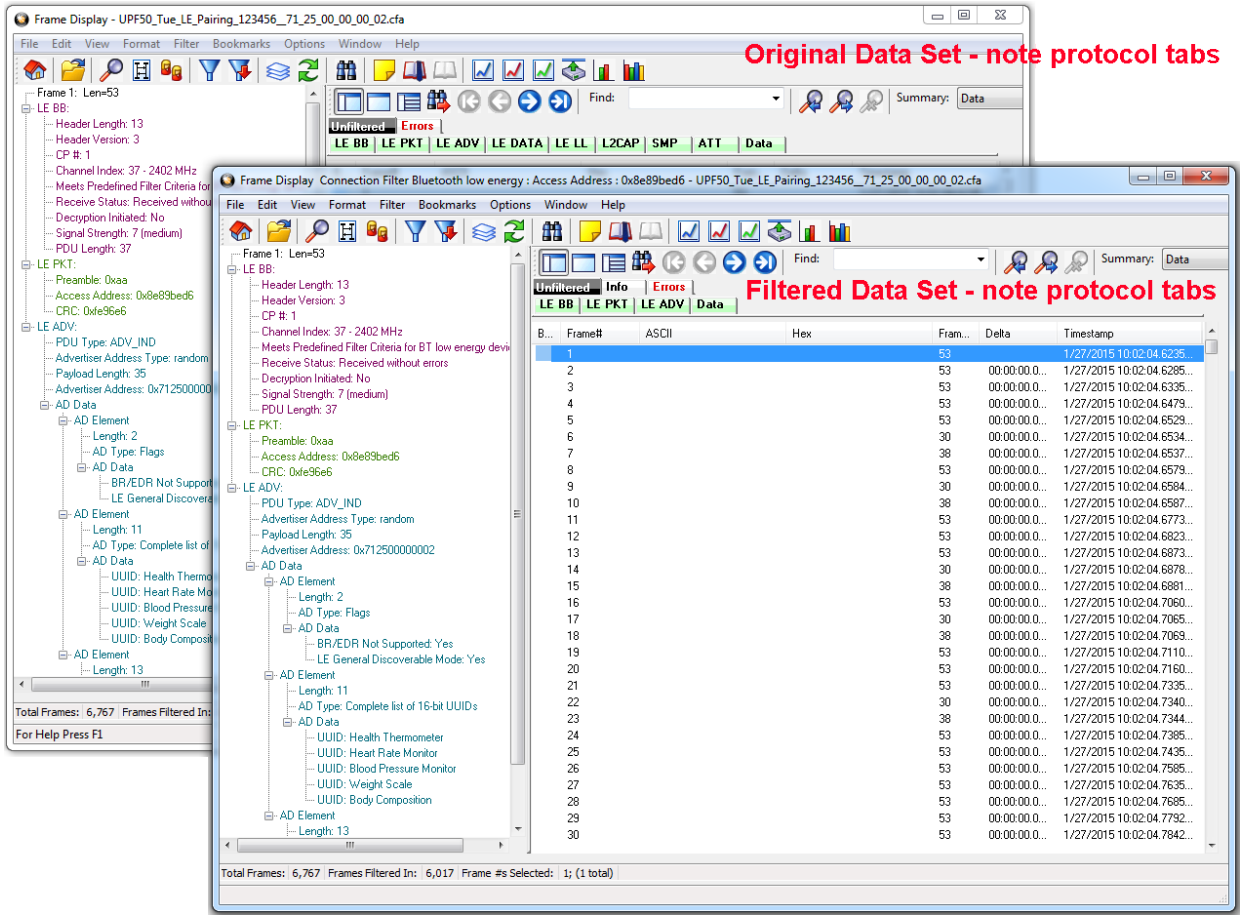


Figure 4.33 - Front Display: Filtered on Access Address 0x8e89bed6

In the figure above is an example Bluetooth low energy data set connection filtered on Access Address = 0x8e89bed6. The Frame Display in the front is the filtered data set. One way to note the difference between the original and the filtered display is to observe the Protocol Tabs. In the filtered display there are four low energy protocol tabs as compared to nine in the original display. This access address connection is not using five of the protocols.

From any open Frame display the user can set another Connection Filter based on the original data set.

Display Example 2: All 802.11 data filtered in

In this example, there is a capture file with Classic *Bluetooth*, *Bluetooth* low energy, and 802.11. To view just the 802.11 data set, 802.11 = All is selected from the right-click pop up menu.

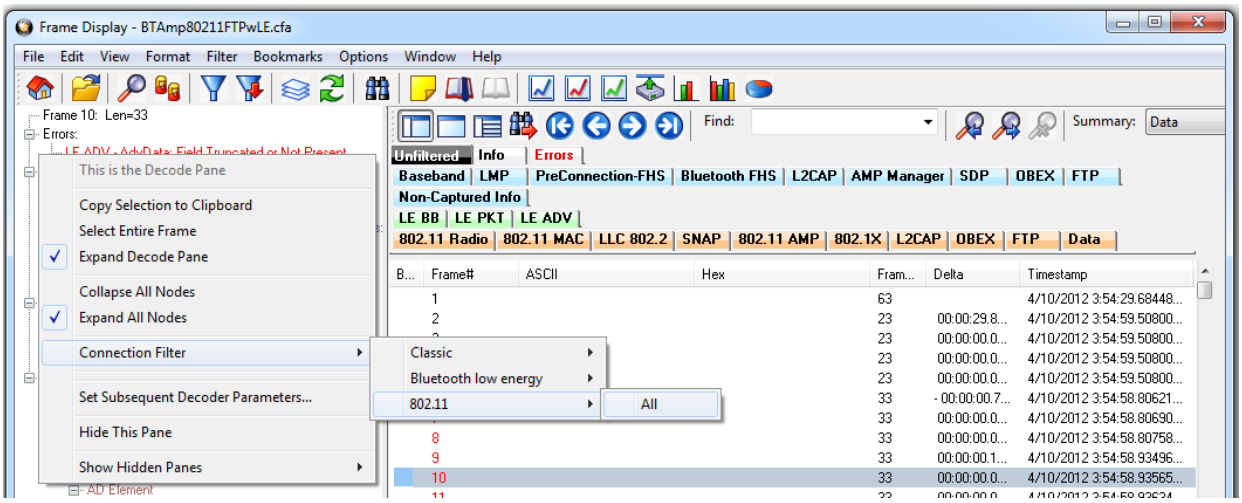


Figure 4.34 - Unfiltered: Capture File with Classic, low energy, and 802.11

When the Frame Display with the filtered 802.11 data set appears, only the Protocol Tabs for 802.11 are present and the tabs for Classic *Bluetooth* and *Bluetooth* low energy have been filtered out.

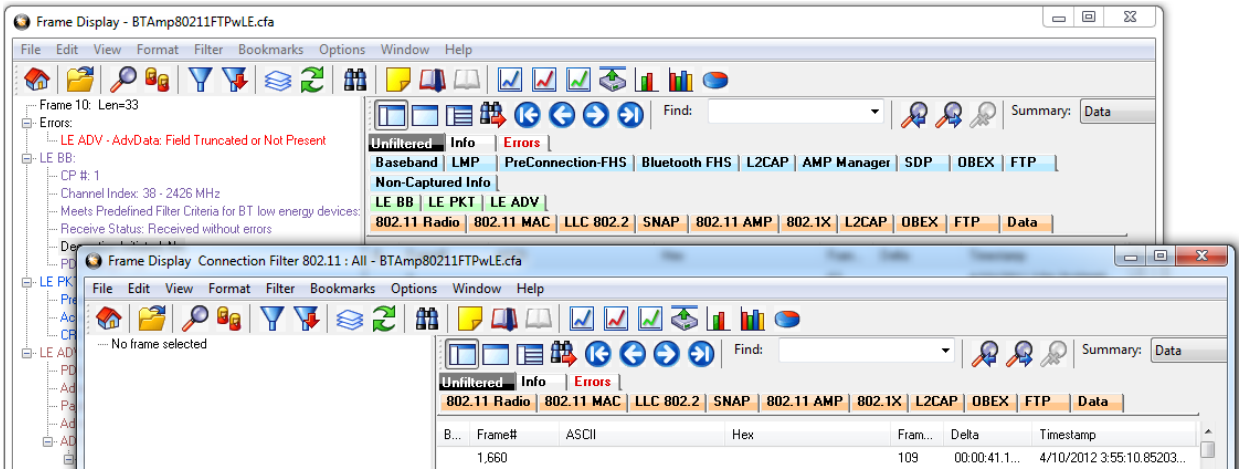

Frame Display - BTAmp80211FTPwLE.cfa
Frame Display Connection Filter 802.11 : All - BTAmp80211FTPwLE.cfa
No frame selected
Find:
Summary:
Data
Unfiltered Info Errors
802.11 Radio 802.11 MAC LLC 802.2 SNAP 802.11 AMP 802.1X L2CAP OBEX FTP Data
B... Frame# ASCII Hex Fram... Delta Timestamp

Figure 4.35 - Connection Filter selecting All 802.11 frames, front

4.4.1.13.3 Protocol Filtering from the Frame Display

4.4.1.13.3.1 Quick Filtering on a Protocol Layer

On the **Frame Display** , click the **Quick Filtering** icon or select **Quick Filtering** from the **Filter** menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

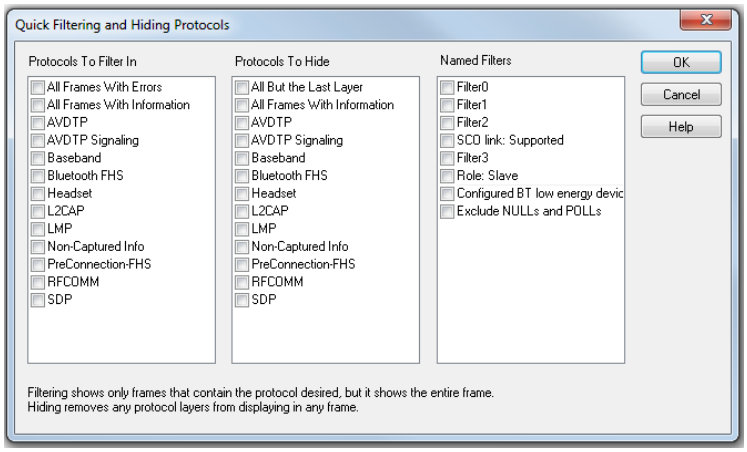


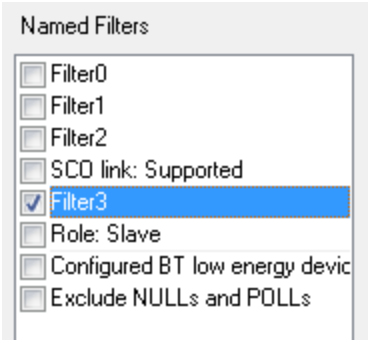
Figure 4.36 - Frame Display Quick Filtering and Hiding Protocols Dialog

The box on the left is **Protocols To Filter In**. When you select the checkbox for a protocol in the **Protocols to Filter In**, the **Summary** pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A **Quick Filter** tab then appears on the **Frame Display**. Changing the filter definition on the **Quick Filter** dialog changes the filter applied on the **Quick Filter** tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**. When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the **Decode**, **Binary**, **Radix**, and **Character** panes. The frames containing that type data will still appear in the **Summary** pane, but not in the **Decode**, **Binary**, **Radix**, and **Character** panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs. When you select the checkbox for the **Name Filters**, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.



With low energy, the Configured BT Low energy devices and Exclude NULLS and POLLs are default named filters.

Check the small box next to the name of each protocol you want to filter in, hide, or **Named Filter** to display.

Then click **OK**

4.4.1.13.3.2 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the **Summary** pane, and the second lets you filter on any protocol discovered on the network so far.

4.4.2 *Bluetooth* Timeline

In addition to the Coexistence View, which displays both Bluetooth® and 802.11 data together, you can also see more information about *Bluetooth* in a separate dialog. The *Bluetooth* **Timeline** displays packet information with an emphasis on temporal information and payload throughput. The timelines also provide selected information from Frame Display.

The timelines provide a rich set of diverse information about *Bluetooth* packets, both individually and as a range. Information is conveyed using text, color, graphic size, line type, and position.

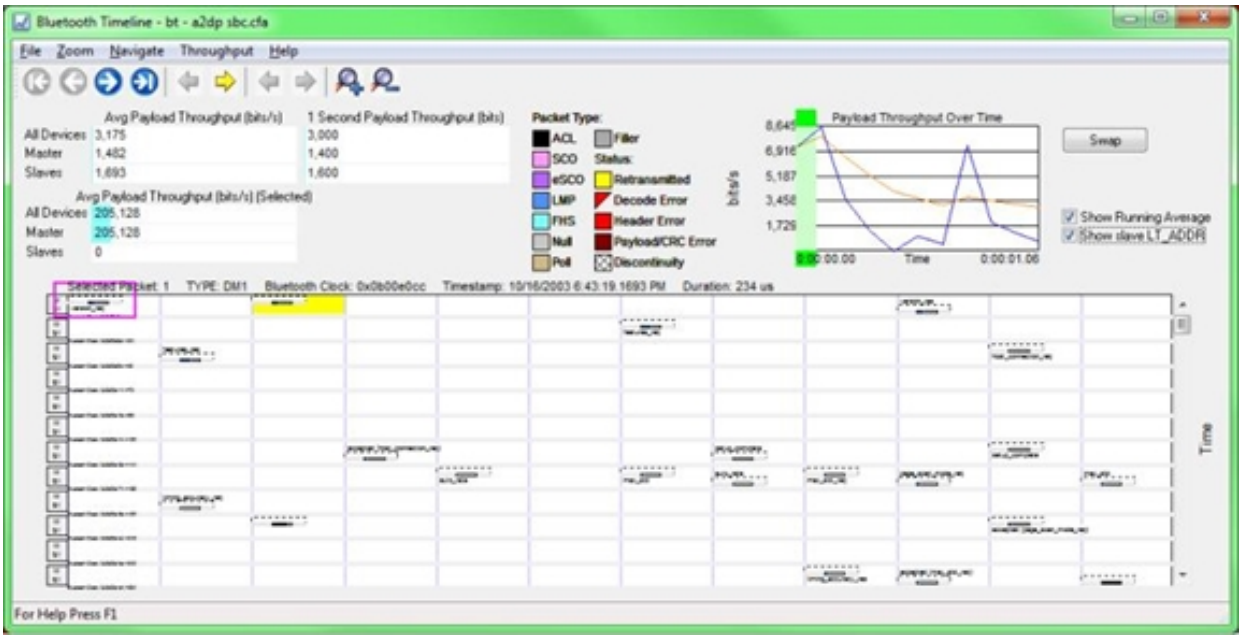


Figure 4.37 - Bluetooth Timeline window

You access the **Bluetooth Timeline** by selecting **Bluetooth Timeline** from the **Control** window **View** menu or by clickingthe **Bluetooth Timeline** icon on the **Control** window toolbar or **Frame Display**.

4.4.2.1 *Bluetooth* Timeline Packet Depiction

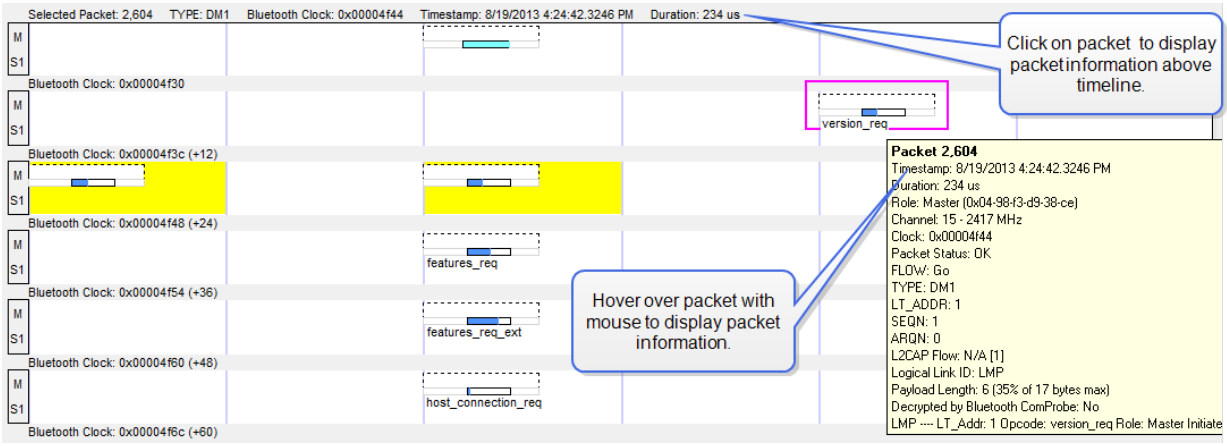
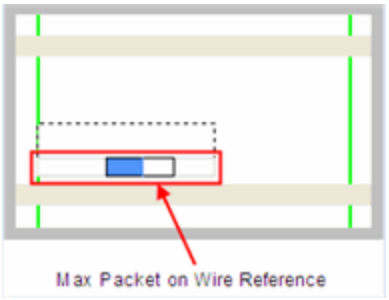

Selected Packet: 2,604 TYPE: DM1 Bluetooth Clock: 0x00004f44 Timestamp: 8/19/2013 4:24:42.3246 PM Duration: 234 us
Click on packet to display packet information above timeline.
Bluetooth Clock: 0x00004f30
version_req
Bluetooth Clock: 0x00004f3c (+12)
Bluetooth Clock: 0x00004f48 (+24)
features_req
Bluetooth Clock: 0x00004f54 (+36)
features_req_ext
Bluetooth Clock: 0x00004f60 (+48)
host_connection_req
Bluetooth Clock: 0x00004f6c (+60)
Hover over packet with mouse to display packet information.
Packet 2,604
Timestamp: 8/19/2013 4:24:42.3246 PM
Duration: 234 us
Role: Master (0x04-98-f3-d9-38-ce)
Channel: 15 - 2417 MHz
Clock: 0x00004f44
Packet Status: OK
FLOW: Go
TYPE: DM1
LT_ADDR: 1
SEQN: 1
ARQN: 0
L2CAP Flow: N/A [1]
Logical Link ID: LMP
Payload Length: 6 (35% of 17 bytes max)
Decrypted by Bluetooth ComProbe: No
LMP ---- LT_Addr: 1 Opcode: version_req Role: Master Initiate

Figure 4.38 - Bluetooth Timeline Packet Depiction with Packet Information Shown

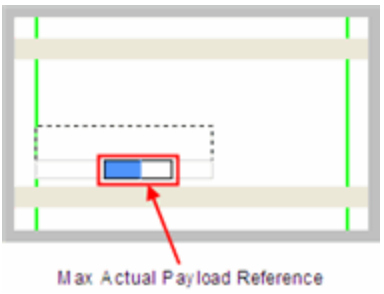
- The timeline shows *Bluetooth* packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M** or **S** depending on the data's role.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet. You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).

A packet is drawn using the following components:

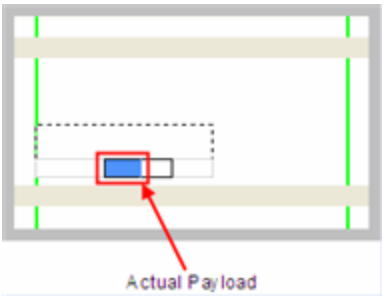
- A “max packet on wire reference” rectangle (light solid lines). This indicates the packet in the air with a max payload.



- A “max actual payload reference” rectangle (dark solid lines). This indicates a max payload as would be extracted by the receiving device (if the payload in the air contains forward error correction (FEC), it is longer than the actual payload). The position of the beginning of the rectangle indicates where the payload begins in time.

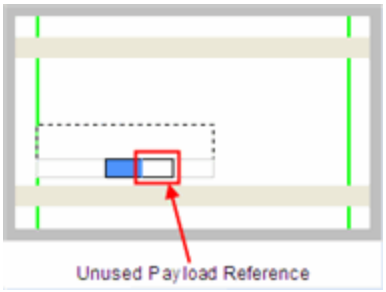


- An “actual payload” colored sub-rectangle (packet category-specific; blue here). This indicates the actual received payload with FEC (if any) removed. It is the beginning portion of the “max actual payload reference” rectangle. If the actual payload is of max size, the entire “max actual payload reference” rectangle is colored.

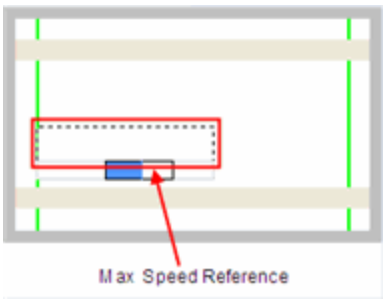


- An “unused payload reference” sub-rectangle (always white). This indicates the unused portion of a maximum payload. It is the remaining portion of the “max actual payload reference” rectangle. The packet in the air does

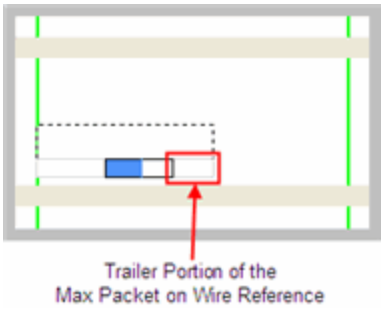
not leave room for this. It is indicated for reference only.



- A “max speed reference” rectangle (dashed lines). This is used to extend the height to that of a 3 Mbits/sec packet, and appears only for packets whose speed is less than that. The packet shown here has a speed of 1 Mbit/sec because the height of the other rectangles is 1/3 of the total height.



- The part of the “max packet on wire reference” rectangle (light solid lines) that trails the “max actual payload reference” rectangle (dark solid lines) is partly packet in the air (if the payload on the wire contained FEC) and partly trailer (CRC, etc). There is always a trailer, so there is always a little space (subject to round off error and pixel granularity) between the ends of the two rectangles.



This table shows how packets are colored:

Table 4.7 - Packet Type Colors

Packet Category	Packet Types	Color
ALC	DM1, DM3, DM5, DH1, 2-DH1, 3-DH1, DH3, 2-DH3, 3-DH3, DH5, 2-DH5, 3-DH5, AUX1	Black
SCO	HV1, HV2, HV3, DV	Pink

Table 4.7 - Packet Type Colors (continued)

Packet Category	Packet Types	Color
eSCO	EV3, 2-EV3, 3-EV3, EV4, EV5, 2-EV5, 3-EV5	Purple
LMP*	DM1, DV	Dark Blue
FHS	FHS	Light Blue
NULL	NULL	Light Gray
POLL	POLL	Light Brown
Filler	Filler provided by ComProbe software	Dark Gray
*LMP is a protocol layer that uses either DM1 or DV packets. If a packet has an LMP layer, the LMP color is used instead of the packet type color.		

This table summarizes the various ways in which packet information is presented:

Table 4.8 - Packet Information Presentation

Information	Text	Color	Graphic size	Position
Packet Type	X			
Packet Category		X		
Protocol	X	X		
Time of occurence	X			X
Source device	X			X
Duration			X	
Size in bytes	X		X	
Size as a percent of max size for that packet type	X		X	
Speed			X	
Status	X		X	

4.4.2.2 *Bluetooth* Timeline Packet Navigation and Selection

- Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous error packet, next or previous retransmitted packet (Bluetooth only), and the first or last packet.

- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet** are enabled, but **Previous Packet** is not.

- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Frame Display**. Selecting a packet activates **Previous Packet**.
- Selecting **Previous Packet** with a packet that is currently not visible, places it in the top row (i.e. the display scrolls up just enough to make it visible).
- Selecting **Next Packet** with a packet that is currently not visible, places it in the bottom row (i.e. the display scrolls down just enough to make it visible).
- Selecting **Previous Packet** or **Next Packet** for a packet that's currently visible selects it without scrolling.
- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline, it is also becomes selected in the **Frame Display**. When multiple packets are selected in the timeline, only one of them is selected in the **Frame Display.**
- The left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.

4.4.2.3 *Bluetooth* Timeline Toolbar

The toolbarbar contains the following:

Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.

Unlock

First Packet

Previous Packet

Next Packet

Last Packet

Previous Retransmitted Packet

Next Retransmitted Packet

Previous Error Packet

Next Error Packet

Zoom In - Click on the icon each time to zoom in from 4800 slots to 12 slots

Zoom Out - Click on the icon each time to zoom out from 12 slots to 4800 slots

Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in Frame Display. Resetting the display may be useful when the most recent throughput values are of interest.

4.4.2.4 *Bluetooth* Timeline Menu Bar

The **Bluetooth Timeline** menu bar contains the following:

Table 4.9 - Bluetooth Timeline Menus

Menu	Selection	Description
File	Reset	Resets Timeline to display beginning at current frame. Available only in Live mode.
	Exit	Closes the timeline window

Table 4.9 - Bluetooth Timeline Menus (continued)

Menu	Selection	Description
Zoom	Zoom In	Displays less of the timeline, but in greater detail. Keyboard Shortcut: (Ctrl +)
	Zoom Out	Displays more of the timeline, in less detail. Keyboard Shortcut: (Ctrl -)
	Zoom In Tool	Displays a magnifying glass icon with a + and an arrow that allows for precise positioning on the timeline. Clicking will show less of the timeline around the point where the tools is clicked.
	Zoom Out Tool	Similar to the Zoom In Tool except with a "-" sign in the magnifying glass, and clicking will show more of the timeline around the point where the tool is clicked.
	Selection Tool	
	12 Slots (3x4)	Display 12 timeline slots arranged in (*row* x *time slots*), that is, three row with 4 time slots.
	36 Slots (6x6)	Displays 36 slots.
	144 Slots (12x12)	Displays 144 slots
	324 Slots (18x18)	Displays 324 slots
	576 Slots (24x24)	Displays 576 slots
	900 Slots (30x30)	Displays 900 slots
	1296 Slots (36x36)	Displays 1296 slots
	1764 Slots (42x42)	Displays 1764 slots
	2304 Slots (48x48)	Displays 2304 slots
	2916 Slots (54x54)	Displays 2916 slots
	3600 Slots (60x60)	Displays 3600 slots
	4356 Slots (66x66)	Displays 4356 slots
	5184 Slots (72x72)	Displays 5184 slots

Table 4.9 - Bluetooth Timeline Menus (continued)

Menu	Selection	Description
Navigate	First Packet	Goes to the first packet. Keyboard Shortcut: Home
	Last Packet	Goes to the last packet. Keyboard Shortcut: End
	Previous Packet	Goes to the packet prior to the currently selected packet. Keyboard Shortcut: Left Arrow
	Next Packet	Goes to the next packet after the currently selected packet. Keyboard Shortcut: Right Arrow
	Previous Retransmitted Packet.	Goes to the previous retransmitted packet from the currently selected packet. If there is no previous retransmission this item is not active.
	Next Retransmitted Packet	Goes to the next retransmitted packet from the currently selected packet. If there are no retransmitted packets following the current selection, this item is not active.
	Previous Error Packet	Goes to the first error packet prior to the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Left Arrow
	Next Error Packet	Goes to the first error packet following the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Right Arrow
	Toggle Display Lock	Available only in Live mode. To prevent timeline scrolling during capture, click on this time and the display will lock in its current position. Capture will continue but the displays will remain static. To resume scrolling during capture, click again on this menu item.
Throughput	Export Payload throughput over time.	Save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph
	Export Object Throughput Stats	Save a comma-separated values (.csv) file that contains information about objects in the timeline. Assumes at most one object transfer per capture.
Help	Help Topics	Displays *Bluetooth* Timeline help topics.

4.4.2.5 *Bluetooth* Timeline Visual Elements

The *Bluetooth* Timeline consists of the following visual elements:

- The timeline shows *Bluetooth* packets within a specific period of time.
- The timeline shows *Bluetooth* packets within a specific period of time.
- The time segments flow left to right and down, following a complete row across. Then you move down to the next row, go across, then down to the next row, just like reading a book, upper left corner to lower right corner.
- Within each row are two divisions: **M** (master) and **S** (Slave). Packets are placed on **M or S** depending on source of the data withing the link.
- Placing the mouse pointer on a packet displays information about that packet in an information box.
- Selecting a packet by clicking on it shows information about that packet above the timeline.
- You can use the arrow keys to move to the next or previous packet.You can select multiple packets by dragging within the timeline or by holding the SHIFT key down while arrowing.
- Using the mouse scroll wheel scrolls the timeline vertically. You can also zoom by using a right click (which displays specific magnification values), using the + and - Zoom tools, or by selecting a value from the Zoom menu.
- Packet height indicates speed (1, 2, or 3 Mbits/sec). Packet length indicates duration (for reference, the duration of a slot is 625-µs). Packet height and length together indicate size (speed times duration).
- Rows of Bluetooth Slots: Each slot begins at the left edge of the vertical blue bar. There are two Bluetooth clocks per slot. Each slot represents 0.000625 seconds, or 625 µs.
- 'M' and 'S' labels: Within each row, master and slave packets are indicated on the left side of the row. By default, all possible slave devices (there can be up to 7) are put on the **S** sub-row, but checking the **Show slave LT_ADDR** checkbox shows all existing slave device sub-rows with numbered labels (some or all of S1, S2, …, S7).
- Bluetooth Clock: The *Bluetooth* clock of the first slot in each row is shown underneath each row.
- Packet Info Line: The packet info line appears just above the timeline and displays information for the currently selected packet(s). If only one packet is selected, this information consists of the **packet number**, **packet type**, *Bluetooth* **clock** (*Bluetooth* only), **Timestamp**, and **Duration**. **Duration** is shown as "Unknown" when the selected packet has an error.

  If multiple packets are selected, this information consists of the packet range, the *Bluetooth* **clock delta** (*Bluetooth* only), the **Timestamp delta**, and **Span**. **Span** is shown as "Unknown" when the last packet in the selected range has an error since its duration is unknown. A user can use these to verify the average throughput calculations.

  Selected packets are bounded by a magenta rectangle. See the Packet Navigation and Selection section.
- Floating Information Window (aka Tooltip): The information window displays when the mouse cursor hovers on a packet (not slot). It persists as long as the mouse cursor stays on the packet or tooltip. For Bluetooth, the tooltip shows the packet number (in bold), the Baseband layer decode from the decode pane of the Frame Display (with the percentage of the Payload Length max added).

  Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.

- Zoom Tools: **Zoom** tools zoom in or out while maintaining the position on the screen of the area under the zoom tool. This makes it possible to zoom in or out for a specific packet or area of the timeline. See the "Zooming" section.
- Packet Status: Packet status is indicated by color codes. A yellow slot indicates a re-transmitted packet, a dark red slot indicates a CRC error, and a small red triangle in the upper-left corner of the packet (not the slot) indicates a decode error.
- Right-Click Menu: The right-click menu provides zooming and tool selection. See the "Zooming" section.
- Graphical Packet Depiction: Each packet within the visible range is graphically depicted. See the "Packet Depiction" section.
- Swap Button: The Swap button switches the position of the Timeline and the Throughput graph.
- Show Running Average: Selecting this check box shows a running average in the Throughput Over Time graph as an orange line.
- Show slave LT_ADDR: Selecting this checkbox displays the Slave LT_ADDR in the timeline row labels

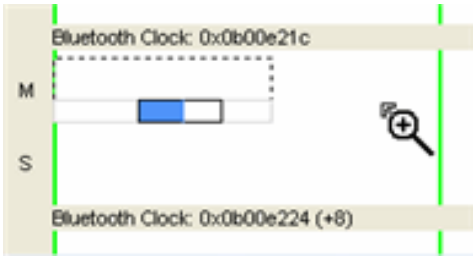
Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

4.4.2.6 *Bluetooth* Timeline Zooming

Zoom features can be accessed from the Zoom menu, clicking a zoom tool on the toolbar, or by right clicking on the **Timeline** window.

A couple of things to remember about Zooming.

- **Zoom** tools accessed using the right click menu allow you to maintain the current position on the screen and precisely zoom in to a specific packet.
- Selecting a **Zoom** icon (+ or -) on the toolbar does not change the pointer to a **Zoom** tool. Each distinct click only zooms in our out.
- **Zoom** tools accessed from the **Zoom** menu have a pointer in the upper-left corner which is useful for specifying the zoom location and bringing up a tool tip of a specific packet.



4.4.2.7 *Bluetooth* Timeline Throughput Displays

In computing throughput, payload is not counted from *Bluetooth* packets that have a CRC error (dark red slot) or that are a retransmission (yellow slot).

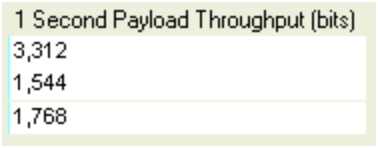
4.4.2.7.1 *Bluetooth* Timeline Average Payload Throughput

The figure depicts the **Throughput** display with the **Average Throughput** indicators in the left column.

Average Throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

- **Average Throughput** is shown as 0 when there is only one packet, because in that case the timestamp difference is 0 and an average cannot be computed.
- **Duration** is the beginning of the first packet to the end of the last packet.
- **Duration** for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- **Average Throughput** is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates relative percentage. Text displays the throughput value.

4.4.2.7.2 *Bluetooth* Timeline 1 Second Throughput Indicators

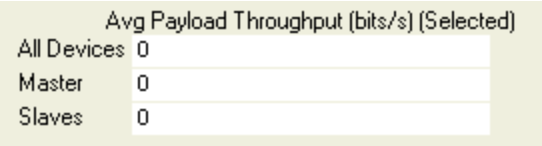


- 1-Second Payload Throughput is the total payload over the most recent one second of duration (This is determined by counting Bluetooth clocks). It is cleared after each discontinuity. A discontinuity is when the Bluetooth clock goes forward more than two (2) seconds or goes backwards any amount. This is caused by either a role switch or Bluetooth clock rollover . The Bluetooth clock count is used instead of timestamp difference because the Bluetooth clock count is precise; however, if timestamp difference were used it would not be necessary to clear the 1-second throughput after each discontinuity. Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.
- 1-second throughput is not an average. It is simply the total payload over the most recent one second of duration. Since it's not an average, it behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small payload by small time), 1-second throughput is very small (since it counts only what it sees and doesn't try to extrapolate).
- A 1-second throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates percentage of max, and text gives the actual throughput.

4.4.2.7.3 Average Payload Throughput (bits/s) (Selected)

The following figure depicts the **Throughput** display with the **Average Payload Throughput (bits/sec) (Selected)** indicators in the left column. This portion of the dialog displays average throughput for a selected packet range when you select a packet from the Timeline.

Average throughput is the total payload over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet. In *Bluetooth*, timestamp difference is used instead of *Bluetooth* clock count because timestamp difference is immune to role switches. However, this can result in inaccuracies when the duration is small enough that a coarse timestamp granularity is significant.

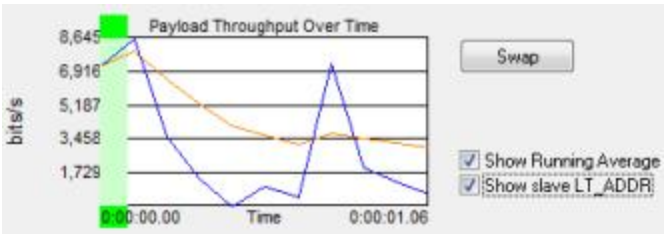


- Duration for average throughput is beginning of first packet to end of last packet. If a single packet is selected, the duration of that packet is used.
- Average throughput can be nonzero when a single packet is selected.
- Average throughput is shown for all devices, master devices, and slave devices.
- A horizontal bar indicates relative percentage. Text displays the throughput value

4.4.2.7.4 *Bluetooth* Payload Throughput Over Time Graph

The following figure depicts the Payload Throughput Over Time graph.

The Payload Throughput Over Time graph shows total payload for each successive time interval. The time interval is initially 0.1 second. Each time the number of throughput elements reaches 100, they are collapsed into a set of 50 by combining adjacent elements and doubling the duration of each element. Collapsing thus occurs as follows:



Collapse count	Time since beginning of session (seconds)	Element duration after collapse (seconds)
1	10	0.2
2	20	0.4
3	40	0.8
4	80	1.6
5	160	3.2
6	320	6.4

and so on...

- Th
e bottom of the graph shows a beginning time and an ending time. The beginning time is relative to the start of the session and initially 0. When packets start wrapping out it becomes the relative time offset of the first available packet. The ending time is always the total time of the session.
- Discontinuities are indicated by vertical dashed lines.
- A green view port indicates the time range corresponding to the visible slots in the timeline. The view port can be moved by clicking elsewhere in the graph or by dragging. Whenever it is moved, the timeline scrolls to match. When the slot range in the timeline changes, the view port moves and resizes as necessary to match.
- The **Swap** button - switches the position of the Timeline and the **Throughput** graph.
- **Show Running Average** - Selecting this check box shows a running average in the **Throughput Over Time** graph as an orange line.
- **Show slave LT_ADDR** - Selecting this checkbox displays the **Slave LT_ADDR** in the timeline row labels.

Comparison with the Coexistence View Throughput Graph

The throughput graphs for Classic *Bluetooth* in the Coexistence View and the *Bluetooth* Timeline can look quite different even though they are plotting the same data. The reason is that the Coexistence View uses timestamps while the *Bluetooth* Timeline uses *Bluetooth* clocks, and they do not always match up exactly. This mismatch can result in the data for a particular packet being included in different intervals in the two throughput graphs, and can have a significant impact on the shapes of the two respective graphs. This can also result in the total duration of the two throughput graphs being different.

Another factor that can affect total duration is that the *Bluetooth* **Timeline**'s throughput graph stops at the last Classic *Bluetooth* packet while the **Coexistence View**'s **Throughput Graph** stops at the last packet regardless of technology.

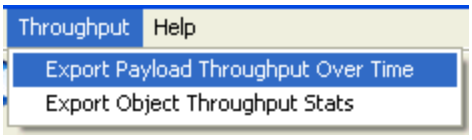
4.4.2.8 Export Payload Throughput Over Time

In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about the **Payload Throughput Over Time** graph. The file contains the following information:

- Sequence Number
- Beginning Packet
- Ending Packet
- Bit Count
- Duration (Secs)
- Bits/Sec
- Running Average (Bits/Sec)

To create the file:

1. Select **Export Payload Throughput Over Time** from the Throughput menu.

   The **Save As** menu appears.

2. Select a location where you want to save the file.

   Note: In live mode, default path name is *C:\Users\Public\Public Documents\Frontline Test Equipment\My Log Files\PayloadThroughputOverTime.csv*. In view mode, default path name is *cfa basepathname with " (PayloadThroughputOverTime).csv"* appended.

3. Enter a **File Name.**
4. Select **Save.**

   The file is saved and you can open it in a simple text editor or database application.

4.4.2.9 Object Throughput Stats File

In the *Bluetooth* **Timeline** you can create and save a comma-separated values (.csv) file that contains information about objects in the timeline. The file contains the following information:

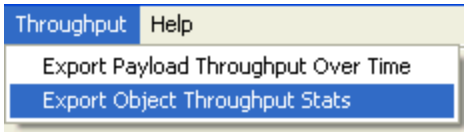
- Name
- Length (bytes)

- Connection Packet Number
- Begin Transfer Packet Number
- End Transfer Packet Number
- Disconnection Packet Number
- Connection Duration
- (Fractional Seconds)
- Transfer Duration
- (Fractional Seconds)
- Connection Throughput (bits/s)
- Transfer Throughput (bits/s)
- Transfer Duration Percentage of Connection Duration
- No Errors Packet Count (Includes Decode Errors) (While Connected)
- Retransmitted Packet Count (While Connected)
- Header Errors Packet Count (While Connected)
- Payload/CRC Errors Packet Count (While Connected)

To create the file:

1. Select **Export Object Throughput Stats** from the Throughput menu.

   The **Save As** menu appears.



2. Select a location where you want to save the file.

   Note: In live mode, the default path name is *C:\Users\Public\Publick Documents\Frontline Test Equipment\My Log Files\ObjectThroughputStats.csv.* In view mode, default path name is *cfa basepathname with " (ObjectThroughputStats).csv"* appended.

3. Enter a **File Name.**
4. Select **Save.**

   The file is saved and you can open it in a simple text editor or database application

4.4.2.10 *Bluetooth* Timeline Discontinuities

The following figure depicts a discontinuity between two packets.

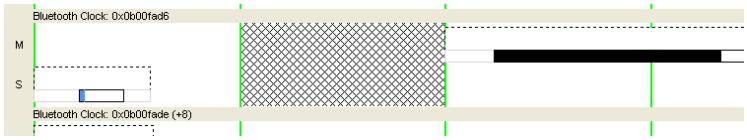
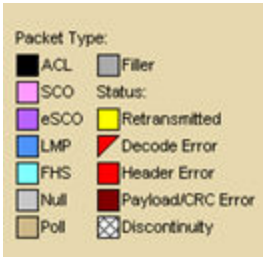


Figure 4.10 *Bluetooth* Timeline Packet Discontinuity, cross-hatched area.

To keep the timeline and the throughput graph manageable, big jumps in the *Bluetooth* clock are not represented linearly. Instead, they are shown as discontinuities. A discontinuity is said to exist when the *Bluetooth* clock goes forward more than two (2) seconds or backwards any amount. A discontinuity is indicated by a cross-hatched slot in the timeline and a corresponding vertical dashed line in the throughput graph. The *Bluetooth* clock can jump forward when capture is paused or when there is a role switch (in a role switch, a different device becomes master, and since each device keeps its own *Bluetooth* clock, the clock can change radically), and backwards when there is a role switch or clock rollover

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

4.4.2.11 Legend



This legend identifies the color coding found in the timeline.

4.4.2.12 *Bluetooth* Timeline: Packets Missing *Bluetooth* Clock

Captured data that is missing the *Bluetooth* clock, such as HCI and BTSnoop, will not display packets. In an instance when the data is missing the clock the *Bluetooth* Timeline will display a message in the Throughput Graph and the Timeline: "Packets without a Bluetooth clock (such as HCI) won't be shown."

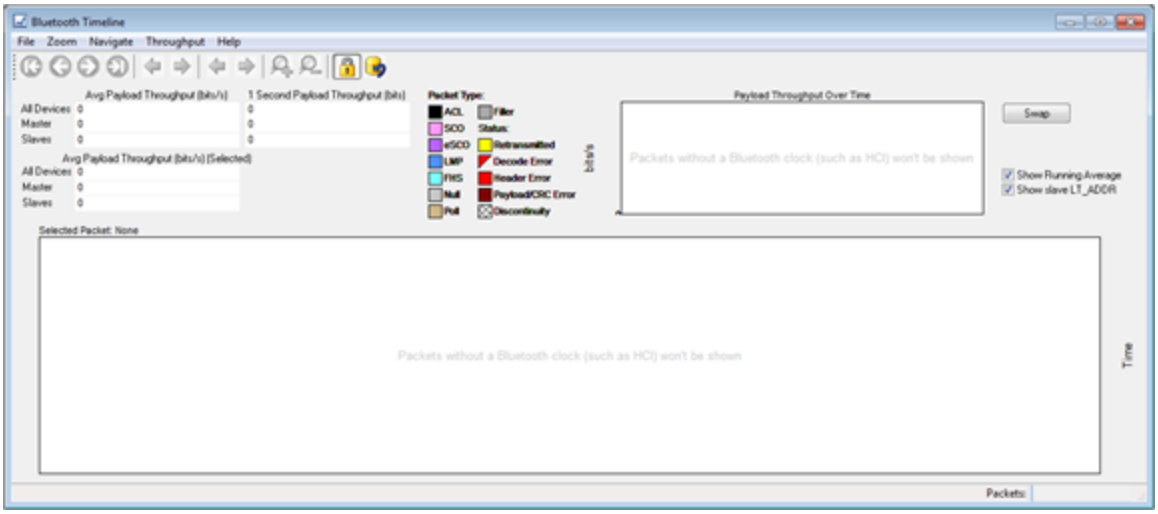

Bluetooth Timeline
File Zoom Navigate Throughput Help
Packets without a Bluetooth clock (such as HCI) won't be shown
Packets:

Figure 4.39 - Missing packets message in timeline pane.

4.4.3 low energy Timeline

The **Bluetooth low energy Timeline** displays packet information with an emphasis on temporal information and payload throughput. The timeline also provides selected information from **Frame Display**.

The timeline provides a rich set of diverse information about low energy packets, both individually and as a range. Information is conveyed using text, color, packet size, and position.

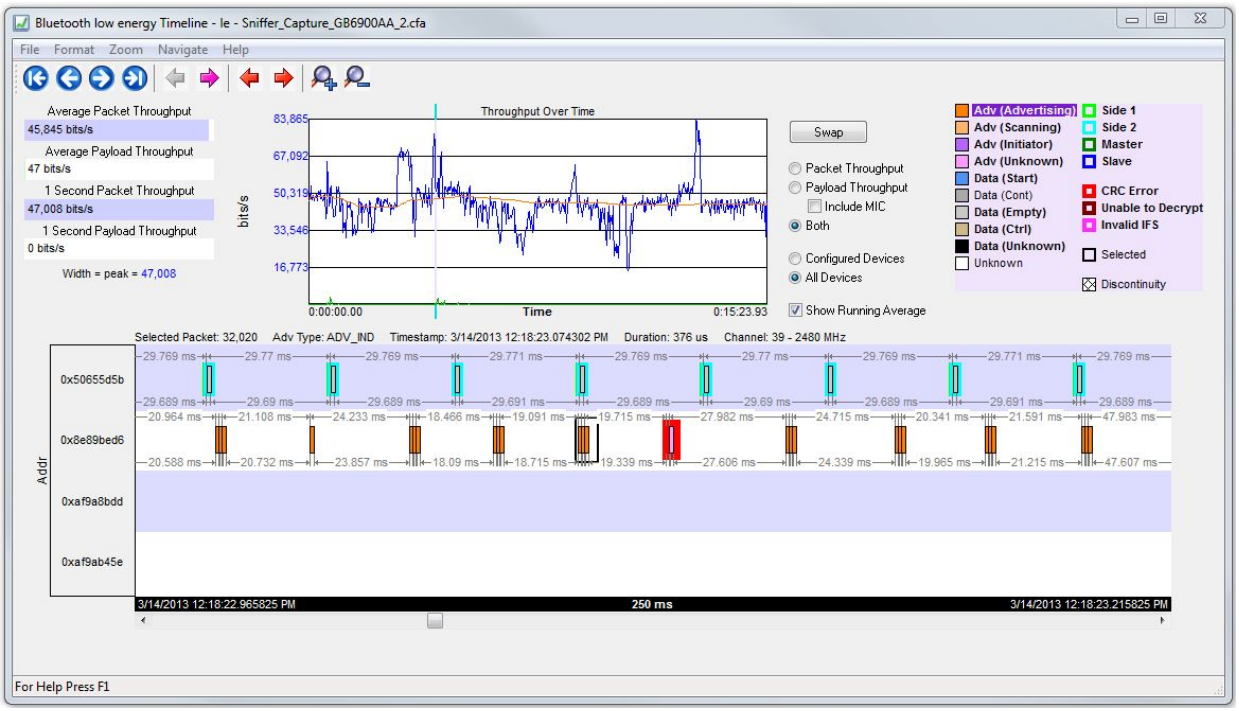


Figure 4.40 - *Bluetooth* **low energy Timeline**

You access the Timeline by selecting **Bluetooth low energy Timeline** from the **View** menu or by pressing the *Bluetooth* low energy Timeline icon on the **Control** window toolbar and **Frame Display** toolbar.

In computing throughput, packets that have a CRC error are excluded.

4.4.3.1 low energy Timeline Toolbar

The toolbar contains the following:

Table 4.11 - *Bluetooth* low energy Timeline Toolbar

Icon	Description
	Lock - The Lock button only appears in live mode and is automatically depressed when the user scrolls.
	Unlock
	First Packet
	Previous Packet
	Next Packet
	Last Packet
	Previous Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 us but less than or equal to 300 µs, it is considered an IFS error.
	Next Interframe Spacing (IFS) Error • Interframe Spacing is considered valid if it is within 150 µs + or – 2us • If the Interframe Spacing is less than 148 us or greater than 152 µs but less than or equal to 300 us, it is considered an IFS error.
	Previous Error Packet
	Next Error Packet
	Zoom In
	Zoom Out

Table 4.11 - Bluetooth low energy Timeline Toolbar (continued)

Icon	Description
	Reset - The Reset button appears only in live mode. Reset causes all packet data up to that point to be deleted from the Packet Timeline display. This does not affect the data in Frame Display. Resetting the display may be useful when the most recent throughput values are of interest.

4.4.3.2 low energy Timeline Menu Bar

The ***Bluetooth*** **low energy Timeline** menu bar contains the following:

Table 4.12 - Bluetooth low energy Timeline Menus

Menu	Selection	Description
File	Reset	Resets Timeline to display beginning at current frame. Available only in Live mode.
	Exit	Closes the timeline window
Format	Show Device Address Rows	Displays rows of packets from sending devices. The source device address will appear on the left of each row.
	Show Radio Rows	Displays rows packets received on radios 0,1, or 2. The radio number will appear on the left of each row.

Table 4.12 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
Zoom	Zoom In	Displays less of the timeline, but in greater detail. Keyboard Shortcut: (Ctrl +)
	Zoom Out	Displays more of the timeline, in less detail. Keyboard Shortcut: (Ctrl -)
	Zoom In Tool	Displays a magnifying glass icon with a + and an arrow that allows for precise positioning on the timeline. Clicking will show less of the timeline around the point where the tools is clicked.
	Zoom Out Tool	Similar to the Zoom In Tool except with a "-" sign in the magnifying glass, and clicking will show more of the timeline around the point where the tool is clicked.
	Selection Tool	
	Single Segment Zoom: Each selection defines the time displayed, "1" segment, and number of 1.25 ms markers withing the segment.	
	2.5 ms (1x2)	Displays one 2.5 ms segment with 2 markers.
	11.25 ms (1x9)	Displays one 11.25 ms segment with 9 markers.
	33.75 ms (1x27)	Displays one 33.75 ms segment with 27 markers.
	125 ms (1x100)	Displays one 125 ms segment with 100 markers.
	437.5 ms (1x350)	Displays one 437.5 ms segment with 350 markers.
	1.875 s (1x1500)	Displays one 1.875 s segment with 1500 markers.
	3.75 s (1x3000)	Displays one 3.75 ms segment with 3000 markers.
	Multiple Segment Zoom: Each selection defines the timeline view port, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "7.5 ms (6 1.25 ms time intervals (3x2))" will display "7.5 ms" of the total timeline in "3" segments of with "2" markers per segment for a total of "6" markers.	
	7.5 ms (6 1.25 ms time intervals (3x2))	3 segments, 2 markers per segment: 1.25 ms x 6 = 7.5 ms total; 1.25 ms x 2 = 2.5 ms per segment.
	22.5 ms (18 1.25 ms time intervals (6x3))	6 segment, 3 markers per segment
	90 ms (72 1.25 ms time intervals (12x6))	12 segments, 6 markers per segment
	202.5 ms (162 1.25 ms time intervals (18x9))	18 segments, 9 markers per segment
	360 ms (288 1.25 ms time intervals (24x12))	24 segments, 12 markers per segment

Table 4.12 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
	562.5 ms (450 1.25 ms time intervals (30x15))	30 segments, 15 markers per segment
	810 ms (648 1.25 ms time intervals (36x18))	36 segments, 18 markers per segment
	1.1025 s (882 1.25 ms time intervals (42x21))	30 segments, 15 markers per segment
	1.44 s (1152 1.25 ms time intervals (48x24))	48 segments, 24 markers per segment
	1.8225 s (1458 1.25 ms time intervals (54x27))	45 segments, 27 markers per segment
	2.25 s (1800 1.25 ms time intervals (60x30))	60 segments, 30 markers per segment
	2.7225 s (2178 1.25 ms time intervals (66x33))	66 segments, 33 markers per segment
	3.24 s (2592 1.25 ms time intervals (72x36))	72 segments, 36 markers per segment
	3.8025 s (30421.25 ms time intervals (78x39))	78 segments, 39 markers per segment
	4.41 s (3528 1.25 ms time intervals (84x42))	84 segments, 42 markers per segment
	5.0625 s (4050 1.25 ms time intervals (90x45))	90 segments, 45 markers per segment

Table 4.12 - Bluetooth low energy Timeline Menus (continued)

Menu	Selection	Description
Navigate	First Packet	Goes to the first packet. Keyboard Shortcut: Home
	Last Packet	Goes to the last packet. Keyboard Shortcut: End
	Previous Packet	Goes to the packet prior to the currently selected packet. Keyboard Shortcut: Left Arrow
	Next Packet	Goes to the next packet after the currently selected packet. Keyboard Shortcut: Right Arrow
	Previous Invalid IFS Packet.	Goes to the previous invalid IFS packet from the currently selected packet. If there is no previous invalid IFS packet this item is not active.
	Next Invalid IFS Packet	Goes to the next invalid IFS packet from the currently selected packet. If there are no invalid IFS packets following the current selection, this item is not active.
	Previous Error Packet	Goes to the first error packet prior to the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Left Arrow
	Next Error Packet	Goes to the first error packet following the current selection. If there are no error packets available, this item is not active. Keyboard Shortcut: Ctrl+Right Arrow
	Selected Packet	Keyboard Shortcut: Enter
	Toggle Display Lock	Available only in Live mode. To prevent timeline scrolling during capture, click on this time and the display will lock in its current position. Capture will continue but the displays will remain static. To resume scrolling during capture, click again on this menu item.
Help	Help Topics	Displays *Bluetooth* low energy Timeline help topics.

4.4.3.3 low energy Timeline Legend

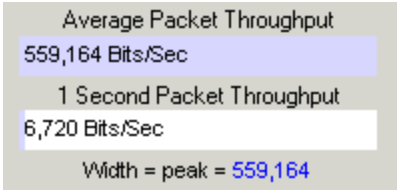
This legend identifies the color coding found in the timeline.

- When you select a packet in the timeline, items in the legend that relate to the packet are highlighted.
- Bold text indicates that the type of packet has been seen in the timeline.

4.4.3.4 Throughput Displays

Throughput is payload over time. There are 3 categories of throughput:

4.4.3.5 Average and 1 Second Packet Throughput



The figure depicts the **Average** and **1 Second Packet Throughput** displays. This display appears when you select the **Packet Throughput** radio button.

- **Average Packet Throughput** is the total packet size over the entire session divided by the total time. Total time is calculated by taking the difference in timestamps between the first and last packet.
- **1-Second Packet Throughput** is the total packet size over the most recent one second.
- **Width = peak =**: This displays the maximum throughput seen so far.
- A horizontal bar indicates percentage of max seen up to that point, and text gives the actual throughput.

4.4.3.6 Average and 1 Second Payload Throughput

The figure depicts the **Average** and **One Second Payload** Throughput display. This display appears when you select the **Payload Throughput** radio button.

- **Average Payload Throughput** is the total payload over the entire session divided by the total time.
- **1-second Payload Throughput**is the total payload over the most recent one second.
- **Width = peak =:** This displays the maximum throughput seen so far.

Note: 1-second throughput behaves differently than average throughput. In particular, while average throughput can be very large with only a couple of packets (since it's dividing small packet or payload size by small time), 1-second throughput can be very small since it divides by an entire one second.

4.4.3.7 Throughput Graph

The following figure depicts the Throughput Graph.

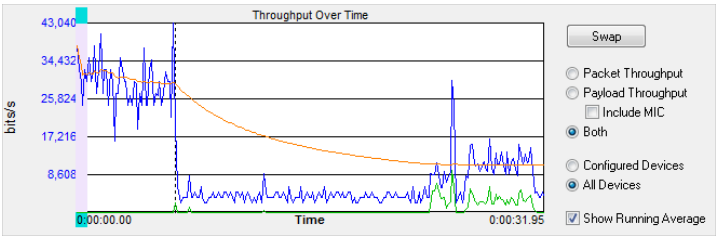


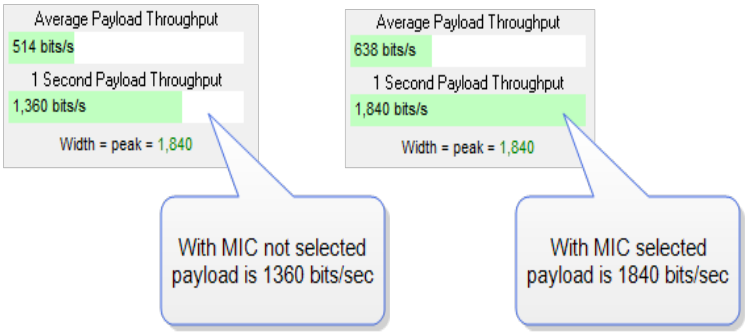
Figure 4.41 - Bluetooth low energy Timeline Throughput Graph

The **Swap** button switches the position of the Timeline and the Throughput graph.

Selecting Throughput Display

- Selecting **Packet Throughput** displays just the **Packet Throughput** in graph form and displays the Average and Average and 1 Second Packet Throughput on the left side of the dialog. The y-axis numbers appear in blue.
- Selecting **Payload Throughput** displays just the **Payload Throughput** in graph form and displays the Average and Average and 1 Second Payload Throughput on the left side of the dialog.. The y-axis numbers appear in green.
- Selecting **Include MIC** will include the transmitted 32 bit Message Integrity Check data in the throughput.

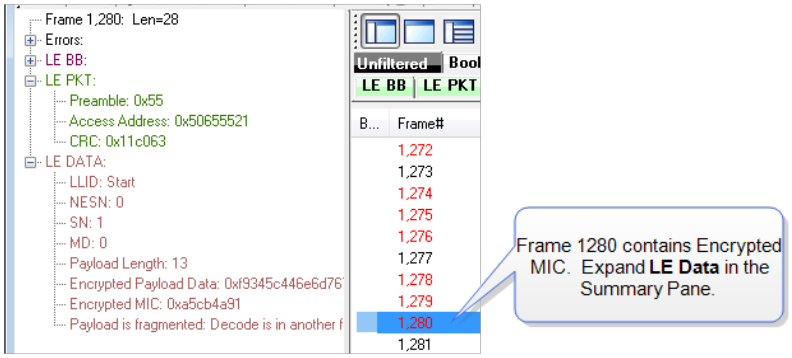
You may want to include Message Integrity Checks in your throughput even though MIC is not application data. MICs are transmitted and you may want to included in the throughput as a measure of how active your radio was.



In this example the 1 Second Payload Throughput is 1,360 bits/sec when **Include MIC** is not checked. By checking the **Include MIC** box the **MIC** data is included in the throughput data and **1 Second Payload Throughput** increases to 1,840 bits/sec. This capture file has 15 MICs in the last second of the file. A MIC is 32 bits for a total of 32 bits X 15 MICs = 480 bits.

The easiest way to view MIC data is to use the **Frame Display**.

1. Using the **Decoder** pane scroll through the frames until LE Data shows "Encrypted MIC".
2. Place the cursor on the Encrypted MIC data and while holding the left



mouse button drag the field to the **Summary** pane.

3. An **Encrypted MIC** column is added to the **Summary** pane.

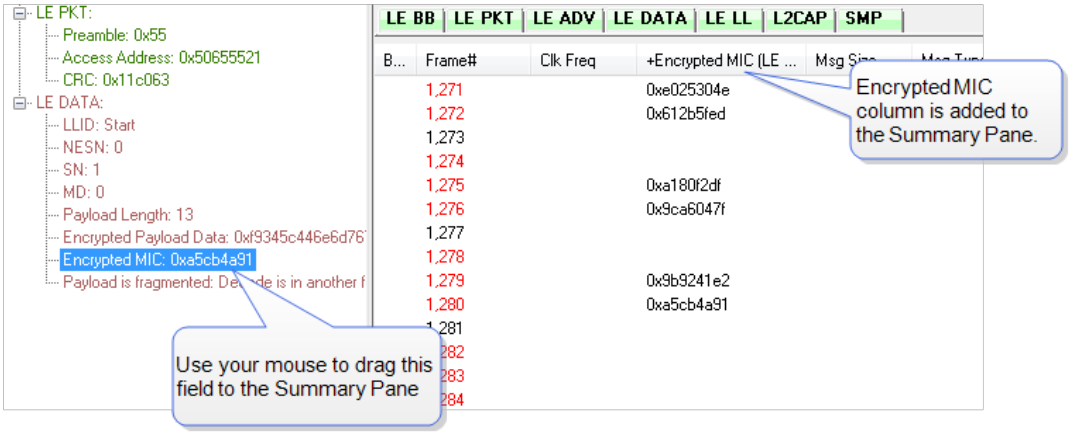


Figure 4.42 - Creating Encrypted MIC in Frame Display Summary pane

4.4.3.8 The Timeline

The **low energy Timeline** shows *Bluetooth* packets within a specific period of time. Time is shown as one or more contiguous segments. Within each segment are one or more source access address or radio rows.

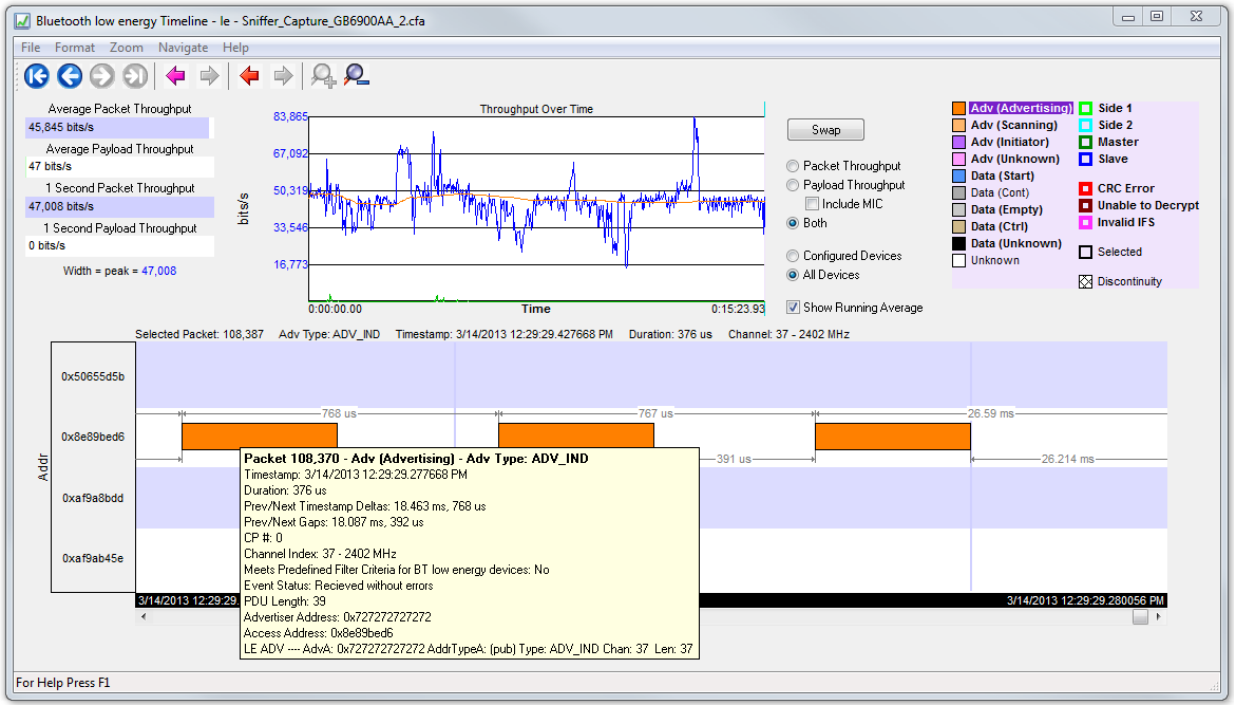


Figure 4.43 - *Bluetooth***low energy Timeline**

4.4.3.9 How Packets Are Displayed

Bluetooth low energy packets are displayed in the low energy timeline in Segments and Rows.

- Segments are "pieces" of the timeline. You can zoom in to show just one segment, or you can zoom out to show multiple segments. In multiple segment displays the segments are contiguous from top to bottom. Refer to the diagram below. The top-most segment contains the beginning timestamp on the left. The timeline proceeds from left to right in a segment, and continues in the next segment down beginning on the left of that segment. If you zoom out to show two segments the viewable timeline appears in those two segments. You will use the scroll bar on the right to scroll through the timeline.

  In a one-segment display the viewable timeline appears in that one segment. You will scroll through the timeline using the scroll bar appearing at the bottom of the timeline display.

- Rows show either the access address of the configured devices or of all discovered devices. Because the segments are contiguous in multiple segment displays, the rows in each segment are identical.

In the following diagram we see a three segment display showing the timeline flow.

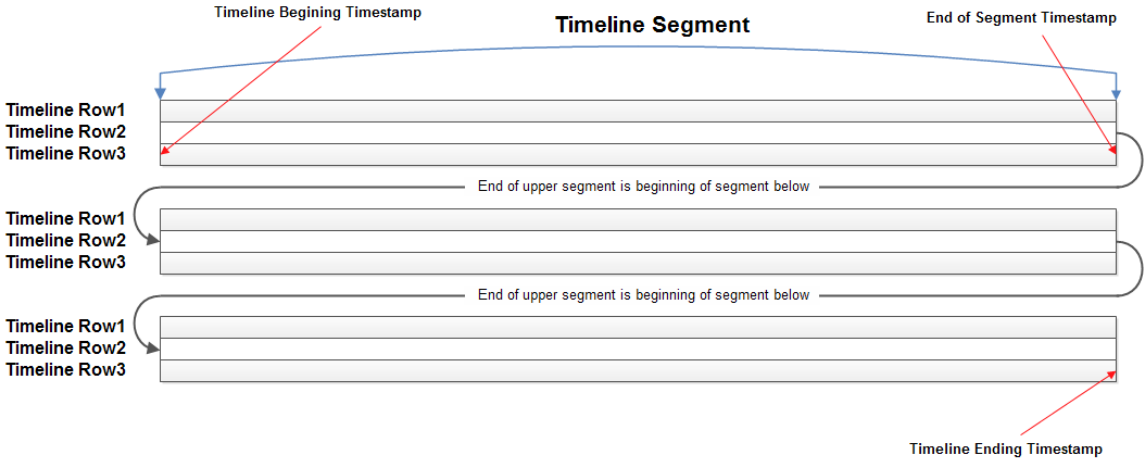
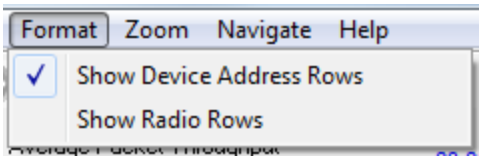


Figure 4.44 - Diagram of low energy Timeline Flow with Segment and Row Relationship

- Rows can display either source device access addresses or the three radios receiving the data..You choose with methods by selecting **Show Device Address Rows** or **Show Radio Rows** from the **Format** menu.

4.4.3.10 Format Menu



Show Device Address Rows will display rows of packets from sending devices. The source device address will appear on the left of each row.

Show Radio Rows will display rows packets received on radios 0,1, or 2. The radio number will appear on the left of each row.

  - The **Addr** rows display packets sent by that access address for all devices or configured devices. You select **All Devices** or **Configured Devices** using the radio buttons.The address shown is the access address for the device.

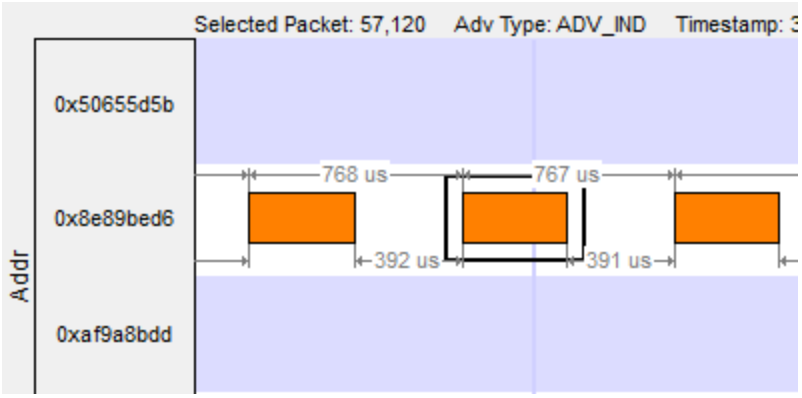


Figure 4.45 - Device Address Rows

- The **Radio** rows display packets received by that radio (0, 1, or 2).

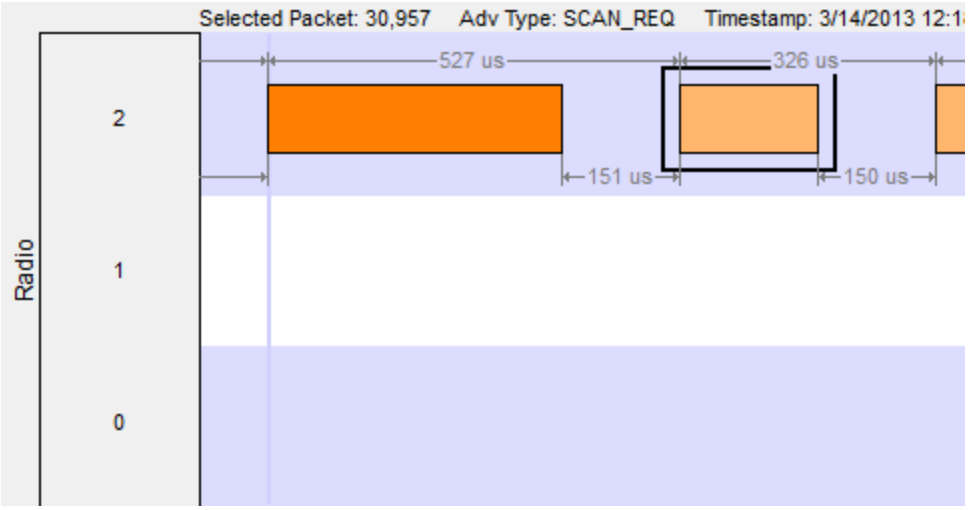


Figure 4.46 - Radio Rows

- The mouse wheel scrolls the timeline horizontally when displaying a single segment, and scrolls vertically when displaying multiple segments
- You can also zoom by using the right-click menu (which displays magnification values), using the + and - Zoom buttons on the toolbar, or by selecting a value from the Zoom menu.
- Packet length indicates duration
- The **Timeline** and **Frame Display** are synchronized so the packet range selected by the user in one is automatically selected in the other. For the selected packet range, the **Timeline** shows various duration values (**Gap**, **Timestamp Delta**, and **Span**), but only if both the first and last packet in the range are available in the **Timeline**. If not, those values are shown as "n/a". Packets that are not displayed in the **Timeline** are Sniffer Debug packets, non-LE packets (e.g. WiFi), and packets that are not from a **Configured Device** the **Configured Devices** radio button is checked.

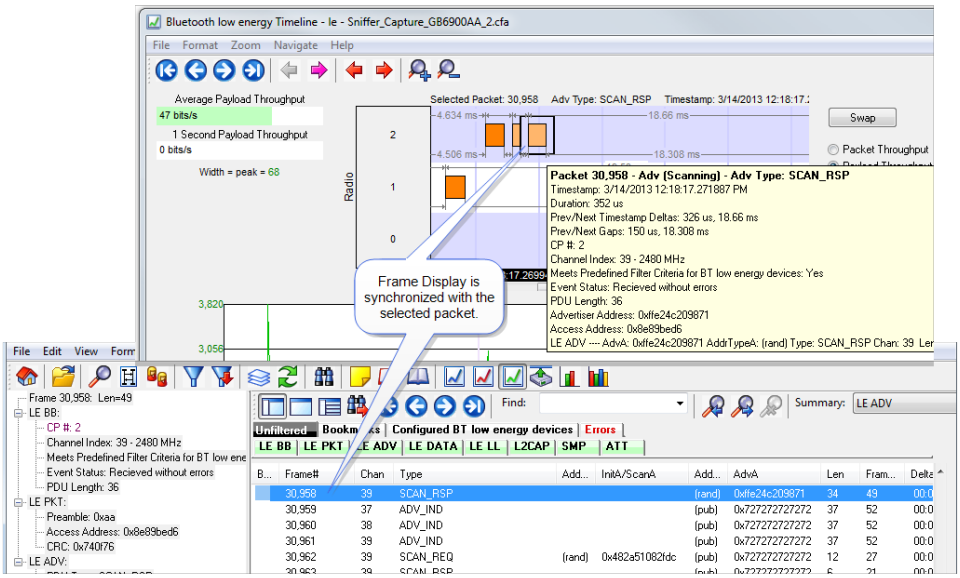

Bluetooth low energy Timeline - le - Sniffer_Capture_GB6900AA_2.cfa
Frame Display is synchronized with the selected packet.

Figure 4.47 - **low energy Timeline** and **Frame Display** Packet Synchronization

4.4.3.11 low energy Timeline Visual Elements

The low energy Timeline consists of the following visual elements:

- Time Markers - Time markers indicated by vertical blue lines are shown at 1.25 ms intervals. The markers are provided to help visualize the timescale and are also useful when using dual-mode chips that do BR/EDR and LE at the same time. Time markers snap to the beginning of the first data packet by default, but they can be snapped to the beginning or end of any packet by right-clicking on a packet and selecting **Align Time Marker to Beginning of Packet** or **Align Time Marker to End of Packet**. All other markers will shift relative to that new reference point.

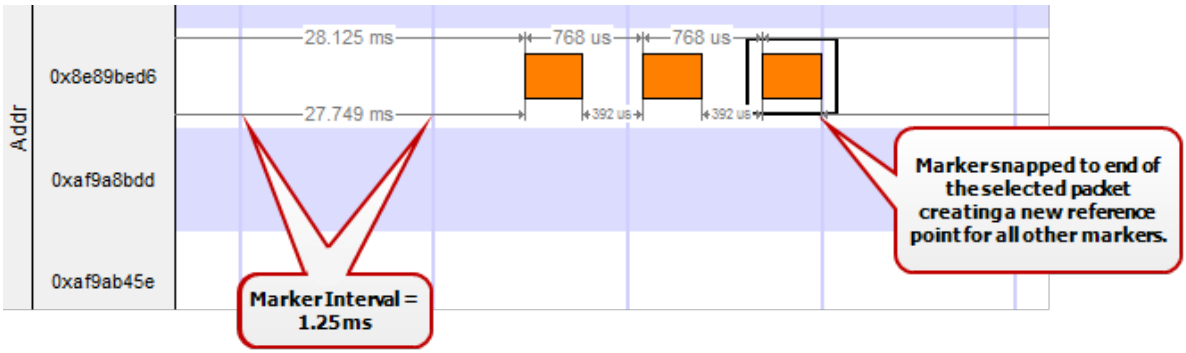


Figure 4.48 - Timeline Markers Shown Snapped to End of Packet

- Timestamp - The beginning and ending timestamp for each segment is displayed beneath each segment. When showing multiple segments the beginning timestamp is the same as the ending timestamp of the

previous segment.

In addition to the timestamps the segment information bar shows the zoom value in the center of the bar.

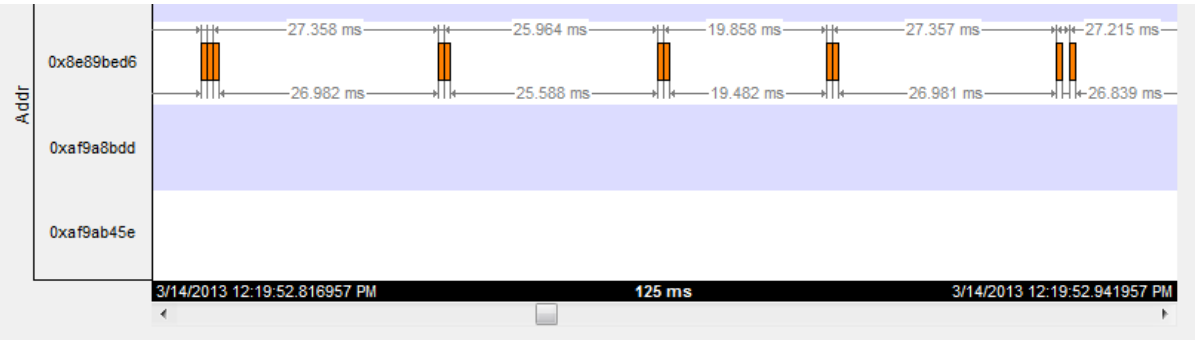


Figure 4.49 - Bluetooth le Timeline Segment Timestamp and Zoom Value

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

- Packet Info Line - The packet info line appears just above the timeline and displays information for the currently selected packet.

Figure 4.50 - Bluetooth le Timeline Packet Info Line

- When you select multiple packets, the info line includes:
  - Gap - duration between the end of the first selected packet and the beginning of the last selected packet.
  - Timestamp Delta - Duration between the beginnings of the first and last packets selected.
  - Span - Duration between the beginning of the first selected packet and the end of the last selected packet

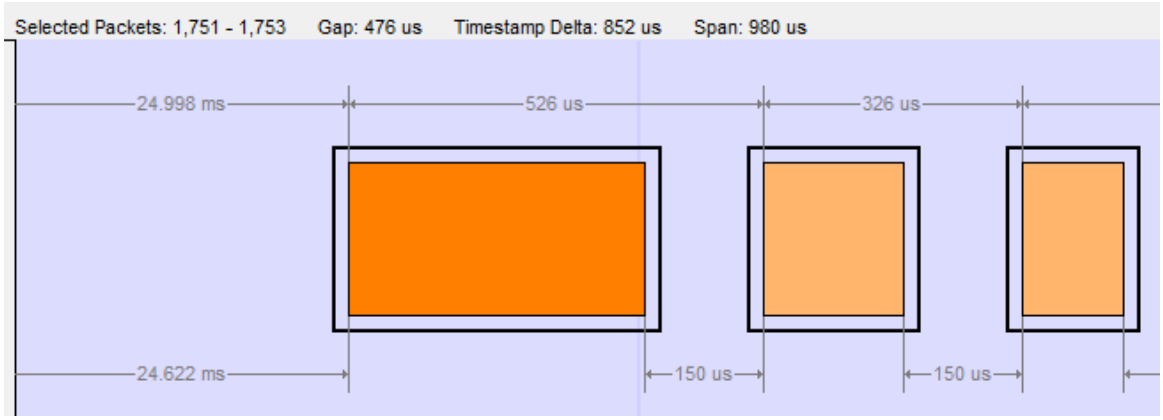
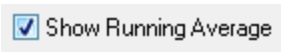


Figure 4.51 - Bluetooth le Timeline Packet Info Line for Multiple Selected Packets

- Floating Information Window (aka Tooltip) - The information window displays when the mouse cursor hovers on a packet. It persists as long as the mouse cursor stays on the packet.
- Discontinuities - Discontinuities are indicated by cross-hatched slots. See the Discontinuities section.
- Packet Status - Packet status is indicated by color codes. Refer to low energy Timeline Legends.
- Right-Click Menu. - The right-click menu provides zooming and time marker alignment.
- Graphical Packet Depiction - each packet within the visible range is graphically depicted. See the Packet Depiction section.
- Swap Button - The Swap button

switches the position of the Timeline and the Throughput graph.
- Show Running Average - -Selecting this check box shows a running average in the Throughput Over Time graph as an orange line 

.

4.4.3.12 low energy Packet Discontinuities

The following figure depicts a discontinuity between two packets.

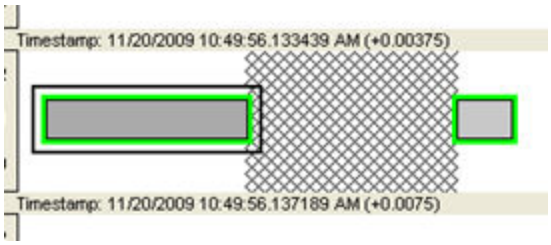


Figure 4.52 - Bluetooth® low energy Packet Discontinuity

To keep the timeline and the throughput graph manageable, big jumps in the timestamp are not represented linearly. Instead, they are shown as discontinuities. A discontinuity exists between a pair of packets when the timestamp delta (the timestamp of the second packet minus the timestamp of the first packet) is (1) more than 4.01 seconds or (2) is negative. The reason that the discontinuity trigger is set at 4.01 seconds is because the maximum connection interval time is 4 seconds.

A discontinuity is indicated by a cross-hatched pattern drawn between two packets and a corresponding vertical dashed line in the throughput graph. When the timestamp delta is greater than 4.01 seconds, the discontinuity is a cosmetic convenience that avoids excessive empty space. When the timestamp delta is negative, the discontinuity is necessary so that the packets can be drawn in the order that they occur.

4.4.3.13 low energy Timeline Navigating and Selecting Data

Buttons, menu items, and keystrokes can be used to go to the next or previous packet, next or previous invalid interframe spacing (IFS), next or previous error packet, and the first or last packet.

- If there is no selected packet in the timeline, **First Packet** , **Next Packet** , and **Last Packet** are enabled, but **Previous Packet** is not.
- A single packet is selected either by clicking on it, navigating to it, or selecting it in the **Frame Display**.
  - Single Segment Navigation:
    - Selecting **Previous Packet** will select the next packet in time (moving back in time to the left) regardless of which row it is on. If the previous packet is not in the display or if a portion of the packet is visible, the display will scroll to the next packet and it will appear selected on the left of the display. The timestamp will change with the scrolling of the display.
    - Selecting **Next Packet** will select the next packet in time (moving forward in time to the right). If the next packet is not in the display, the display will scroll to the next packet and it will appear selected on the right of the display. The timestamp will change with the scrolling of the display.
  - Multiple Segment Navigation:
    - Selecting **Previous Packet** will select the next packet moving back in time (to the left) on the segment and will select the previous packet regardless of which or segment it is in.

      If the selected packet overlaps with the previous segment, the display will show the packet selected in both segments.

      If the previous packet is not shown in the timeline display or a portion of the packet is displayed,the display will move the view port back in time and will display the selected packet in the top segment on the left edge. Each segment's timestamps will synchronously change as the view port scrolls backwards in time.
    - Selecting Next Packet will select the next packet moving forward in time (to the right)on the to the next packet regardless of which row or segment it is in.

      If the next packet overlaps on a following segment, the display will show the packet selected in both segments.

      If the next packet is not shown in the timeline display on any segment or a portion of the packet is displayed, the display will move the view port forward in time and will display the selected packet in the bottom segment on the right edge. Each segment's timestamps will synchronously change as the view port scrolls forward in time. All subsequent selected next packets will appear on the right of the bottom segment.

- Multiple packets are selected either by dragging the mouse or by holding down the shift key while navigating or clicking.
- When a single packet is selected in the timeline it is also becomes selected in the **Frame Display**. When multiple packets are selected in the timeline, only one of them is selected in the **Frame Display**.
- The keyboard left arrow key goes to the previous packet. The right arrow key goes to the next packet. The Ctrl-left arrow key goes to the previous error packet. The Ctrl-right arrow key goes to the next error packet.
- The mouse scroll wheel will scroll the timeline as long as the cursor is in the dialog.

4.4.3.14 low energy Timeline Zooming

Zoom features can be accessed from the **Bluetooth low energy Timeline Zoom** menu by right-clicking on the **Timeline** window.

A couple of things to remember about Zooming.

- Zooming using the toolbar buttons in a single segment display is relative to the center of the display. That is as you zoom out those packets on the left and right halves will move closer to the center. If you zoom in, those packets in the left and right halves will move towards the left and right edges respectively.
- Zooming using the toolbar buttons in a multiple segment display is relative to the number of segments. If you have a single display and zoom out they will become two segments, then three segments, then six, and so forth.
- Selecting a Zoom icon (+ or -) on the toolbar zooms in our out.
- The current Zoom setting is shown in the center of the timeline segment information bar at the bottom of each timeline segment.
- If you are in multiple segments the segment information bar will show the zoom level with the text " (Contiguous time segment *x/n*)" where "*x*" is 1,2, 3… segment and "*n*" is the total number of segments. For example: :"(Contiguous time segment 2/3)".

4.4.3.15 Zoom menu

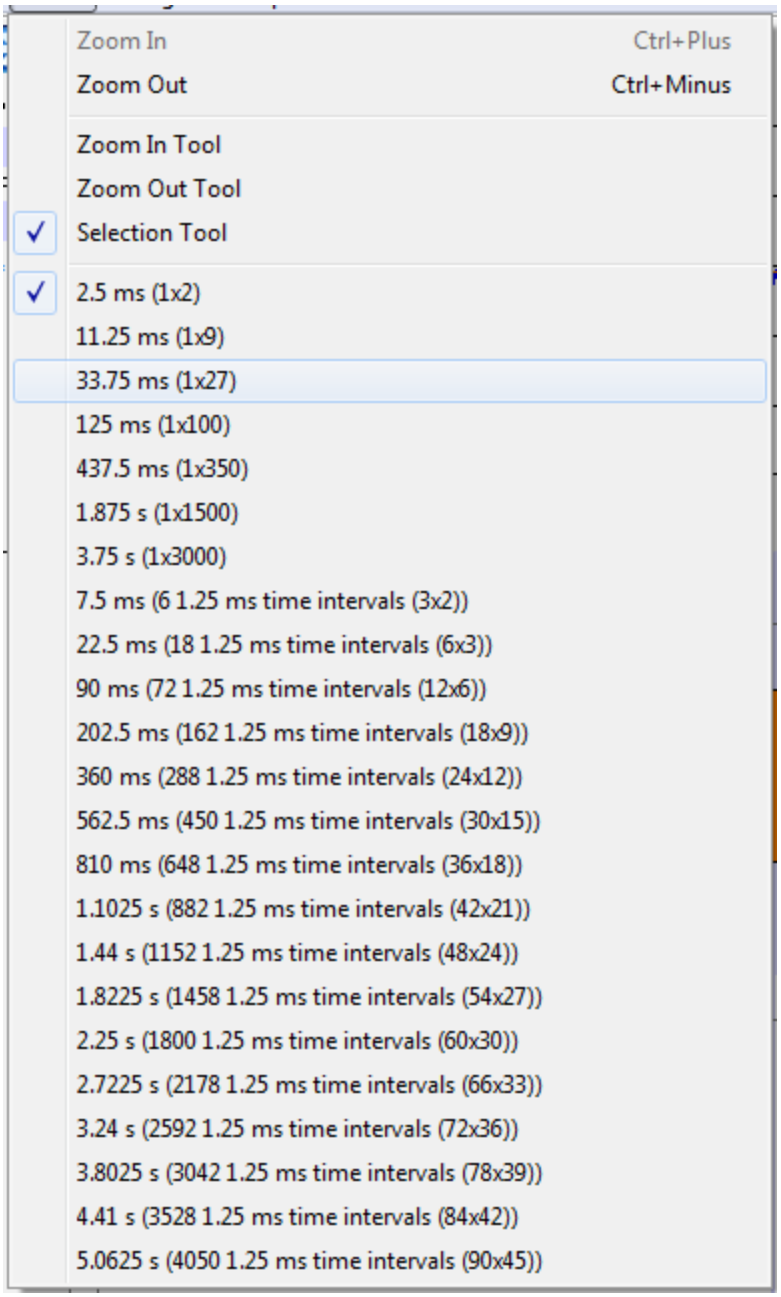
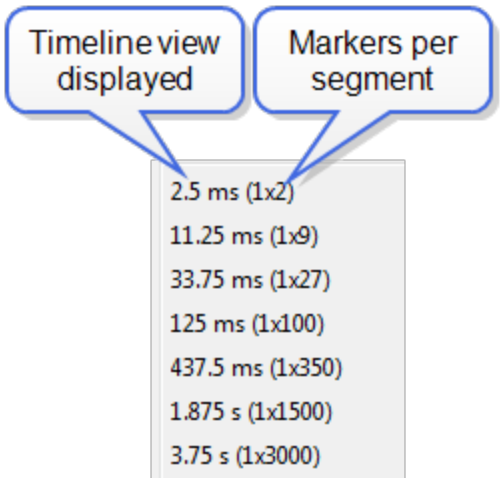

Zoom In Ctrl+Plus
Zoom Out Ctrl+Minus
Zoom In Tool
Zoom Out Tool
Selection Tool
2.5 ms (1x2)
11.25 ms (1x9)
33.75 ms (1x27)
125 ms (1x100)
437.5 ms (1x350)
1.875 s (1x1500)
3.75 s (1x3000)
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time intervals (30x15))
810 ms (648 1.25 ms time intervals (36x18))
1.1025 s (882 1.25 ms time intervals (42x21))
1.44 s (1152 1.25 ms time intervals (48x24))
1.8225 s (1458 1.25 ms time intervals (54x27))
2.25 s (1800 1.25 ms time intervals (60x30))
2.7225 s (2178 1.25 ms time intervals (66x33))
3.24 s (2592 1.25 ms time intervals (72x36))
3.8025 s (3042 1.25 ms time intervals (78x39))
4.41 s (3528 1.25 ms time intervals (84x42))
5.0625 s (4050 1.25 ms time intervals (90x45))

Figure 4.53 - low energy Timeline Zoom menu

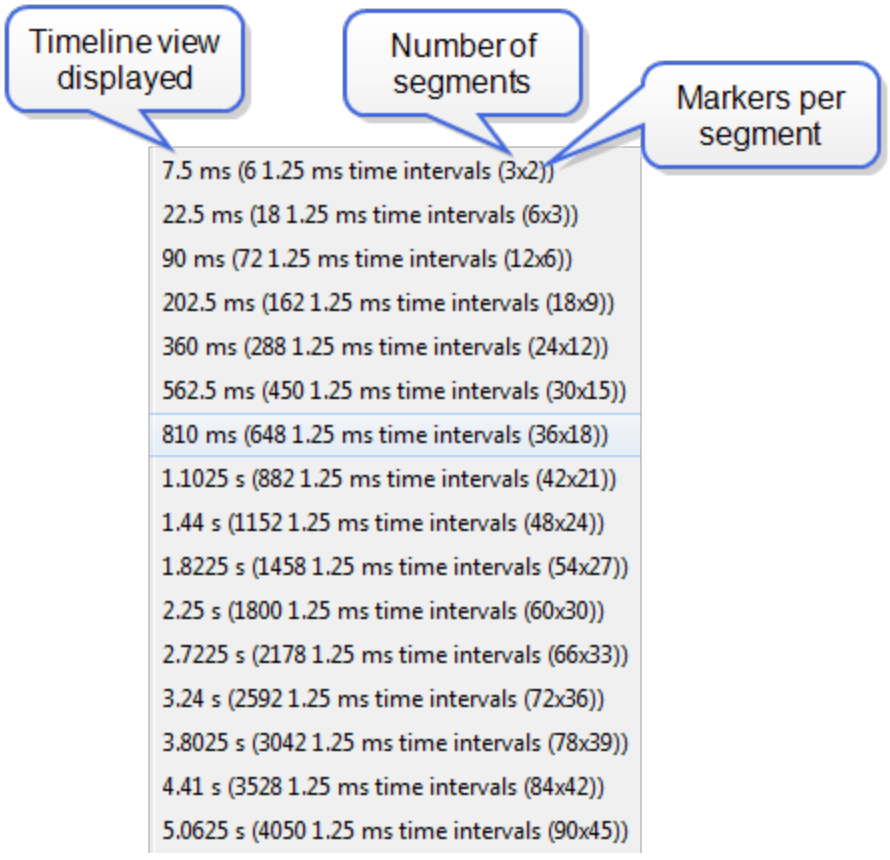
4.4.3.16 Single Segment Zoom



Zoom Menu Single Segment: Each selection defines the timeline displayed, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "33.75 ms (1x27)" will display "33.75 ms" of the throughput graph in "1" segment with "27" markers.

The scroll bar at the bottom of the segment will scroll the throughput graph view port.

4.4.3.17 Multiple Segments


Timeline view displayed
Number of segments
Markers per segment
7.5 ms (6 1.25 ms time intervals (3x2))
22.5 ms (18 1.25 ms time intervals (6x3))
90 ms (72 1.25 ms time intervals (12x6))
202.5 ms (162 1.25 ms time intervals (18x9))
360 ms (288 1.25 ms time intervals (24x12))
562.5 ms (450 1.25 ms time intervals (30x15))
810 ms (648 1.25 ms time intervals (36x18))
1.1025 s (882 1.25 ms time intervals (42x21))
1.44 s (1152 1.25 ms time intervals (48x24))
1.8225 s (1458 1.25 ms time intervals (54x27))
2.25 s (1800 1.25 ms time intervals (60x30))
2.7225 s (2178 1.25 ms time intervals (66x33))
3.24 s (2592 1.25 ms time intervals (72x36))
3.8025 s (3042 1.25 ms time intervals (78x39))
4.41 s (3528 1.25 ms time intervals (84x42))
5.0625 s (4050 1.25 ms time intervals (90x45))

Zoom Menu Multiple Segment: Each selection defines the timeline view port, the number of segments, and number of 1.25 ms markers withing the segment. For example, selecting "7.5 ms (6 1.25 ms time intervals (3x2))" will display "7.5 ms" of the total timeline in "3" segments of with "2" markers per segment for a total of "6" markers.

The scroll bar at the left of the segments will scroll the view through the timeline.

4.4.4 Coexistence View

The **Coexistence View** displays Classic *Bluetooth*, *Bluetooth* low energy, and 802.11 packets and throughput in one view. You access the **Coexistence View** by clicking its button in the **Control** window or **Frame Display** toolbars, or **Coexistence View** from the **View** menus.

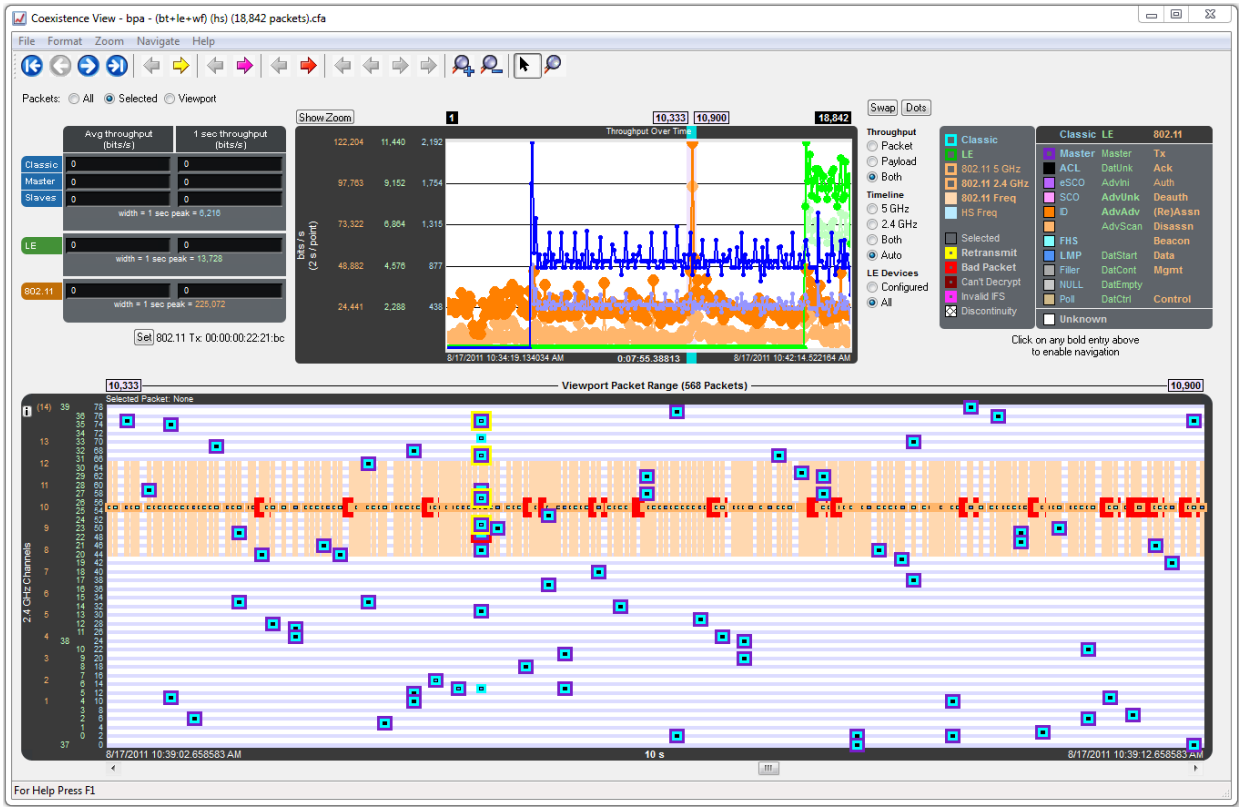


Figure 4.54 - Coexistence View Window

4.4.4.1 Coexistence View - Toolbar

Figure 4.55 - Coexistence View Toolbar

The toolbar contains the following selections:

Table 4.13 - Coexistence View Toolbar icons

Icon	Description
	Move to the first packet.
	Move to the previous packet.
	Move to the next packet.
	Move to the last packet.
	Move to the previous retransmitted packet.
	Move to the next retransmitted packet
	Move to the previous invalid IFS for *Bluetooth* low energy.
	Move to the next invalid IFS for *Bluetooth* low energy.
	Move to the previous bad packet.
	Move to the next bad packet.
	Move to the first packet of the type selected in the legend.
	Move to the previous packet of the type selected in the legend
	Move to the next packet of the type selected in the legend.
	Move to the last packet of the type selected in the legend.
	Zoom in.
	Zoom out.
	Scroll cursor.

Table 4.13 - Coexistence View Toolbar icons (continued)

Icon	Description
	When selected the cursor changes from Scroll to a context-aware zooming cursor. Click on normal cursor to remove the zooming cursor.
	Zooming cursor.
	Scroll Lock/Unlock during live capture mode.
	Reset during live capture mode. Clears the display.

4.4.4.2 Coexistence View - Throughput Indicators

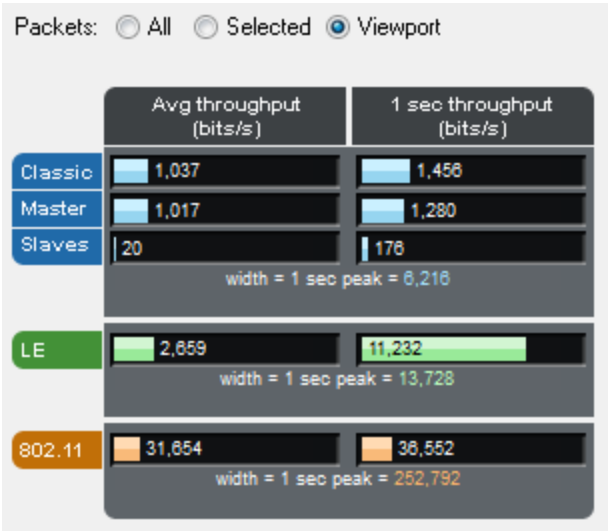


Figure 4.56 - Coexistence View Throughput Indicators

Throughput indicatorsshow average throughput and 1 second throughput for Classic Bluetooth® (all devices, master devices, and slave devices are each shown separately), *Bluetooth* low energy, and 802.11.

4.4.4.3 Throughput

Throughput is total packet or payload size in bits of the included packets divided by the duration of the included packets, where:

- *Packet size* is used if the Packet or Both radio button is selected in the Throughput group.
- *Payload size* is used if the Payload radio button is selected in the Throughput group.
- *Included packets* are defined separately for each of the radio buttons that appear above the throughput indicators.
- *Duration of the included packets* is measured from the beginning of the first included packet to the end of the last included packet.

4.4.4.4 Radio Buttons

The radio buttons above the throughput indicators specify which packets are *included*. Radio button descriptions are modified per the following:

- *Bluetooth* low energy packets from non-configured devices are excluded if the **Configured** radio button in the LE Devices group is selected.

- **Frame Display** filtering has no effect here in that packets that are filtered-out in **Frame Display** are still used here as long as they otherwise meet the criteria for each radio button as described below.

4.4.4.5 All radio button

All packets are used for average throughput, and packets occurring in the last 1 second of the session are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

4.4.4.6 Selected radio button

Selected packets (the selected packet range is shown in the timeline header) are used for average throughput, and packets in the 1 second duration ending at the end of the last selected packet are used for 1 second, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

Figure 4.14 Timeline Header Showing Selected Packets

4.4.4.7 Viewport radio button

The viewport is the purple rectangle in the **Throughput Graph** and indicates a specific starting time, ending time, and resulting duration. Packets that occur within that range of time are used for average throughput, and packets in the 1 second duration ending at the end of the last packet in the viewport time range are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

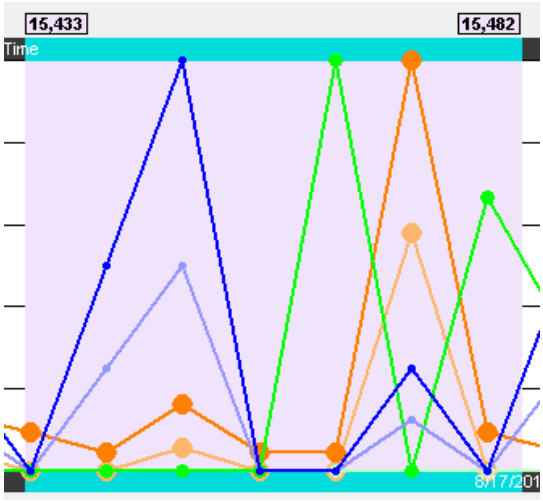


Figure 4.57 - **Throughput Graph** viewport.

4.4.4.8 Indicator width

The width of each indicator is the largest 1 second throughput seen up to that point for that technology (Classic *Bluetooth*, *Bluetooth* low energy, or 802.11), where the 1 second throughput is calculated anew each time another packet is received. The 1 second throughput indicator will never exceed this width, but the average throughput indicator can. For example, the image below has a large average throughput because the Selected radio button was selected and a single packet was selected, and the duration in that case is the duration of the single packet, which makes for a very small denominator in the throughput calculation. When the average throughput exceeds the indicator width, a plus sign (+) is drawn at the right end of the indicator.

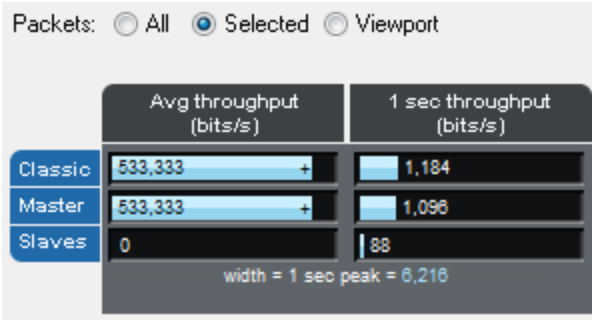


Figure 4.58 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded.

Figure 4.59 - A single selected packet

4.4.4.9 Coexistence View - Throughput Graph

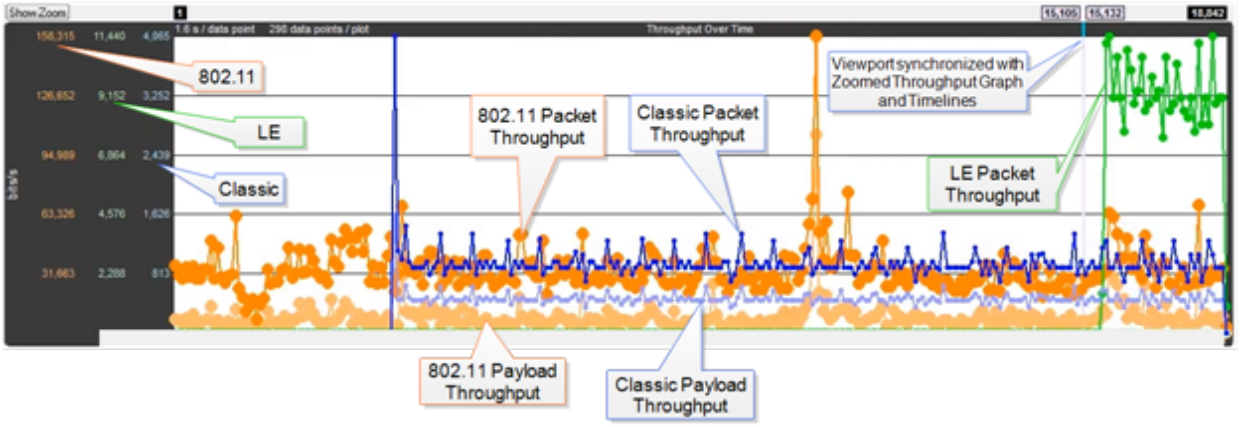


Figure 4.60 - Coexistence View Throughput Graph

The **Throughput Graph** is a line graph that shows packet and/or payload throughput over time as specified by the radio buttons in the Throughput group. If the **Both** radio button is selected, packet and payload throughput are shown as two separate lines for each technology. The payload throughput line is always below the packet throughput line (unless both are 0).

The data lines and y-axis labels are color-coded: Blue = Classic Bluetooth® , Green = *Bluetooth* low energy, Orange = 802.11. Each data point represents a duration which is initially 0.1 s. Each time the number of data points per line reaches 300, the number of data points per line is halved to 150 and the duration per data point is doubled. The duration per data point thus progresses from 0.1 s to 0.2 s to 0.4 s to 0.8 s and so on.

4.4.4.10 Throughput Graph Y-axis labels

The y-axis labels show the throughput in bits per second. From left-to-right the labels are for 802.11, *Bluetooth* low energy, and Classic *Bluetooth*. The duration of each data point must be taken into account for the y-axis label's value to be meaningful. For example, if a data point has a duration of 0.1 s and a bit count of 100, it will have a throughput of 1,000 bits/s, and the y-axis labels will be consistent with this.

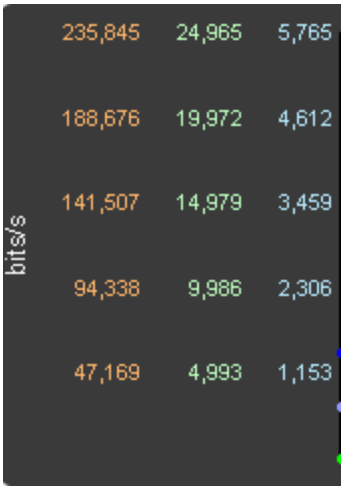


Figure 4.61 - **Throughput Graph** y-axis labels.

4.4.4.11 Excluded packets

Retransmitted packets and bad packets (packets with CRC or Header errors) are excluded from throughput calculations.

4.4.4.12 Tooltips

Placing the mouse pointer on a data point shows a tooltip for that data point. The tooltip first line shows the throughput, the throughput type (packet or payload), and the technology. Subsequent lines show the bit count, the duration of the data point, the packet range of that duration (only packets of the applicable technology from that packet range are used for the throughput calculation), and the number of the data point (which is 0 for the first data point in each line).

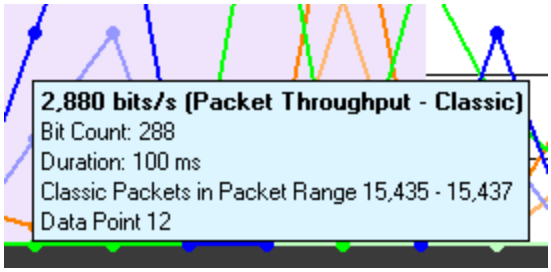

2,880 bits/s (Packet Throughput - Classic)
Bit Count: 288
Duration: 100 ms
Classic Packets in Packet Range 15,435 - 15,437
Data Point 12

Figure 4.62 - Data point tooltip

The Throughput graph tool tips can be shown in the upper-left corner of your computer screen to provide an unobstructed view. Refer to Relocating Tool Tips.

4.4.4.13 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s. This value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s. A discontinuity is drawn as a vertical dashed line. A discontinuity for a

timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

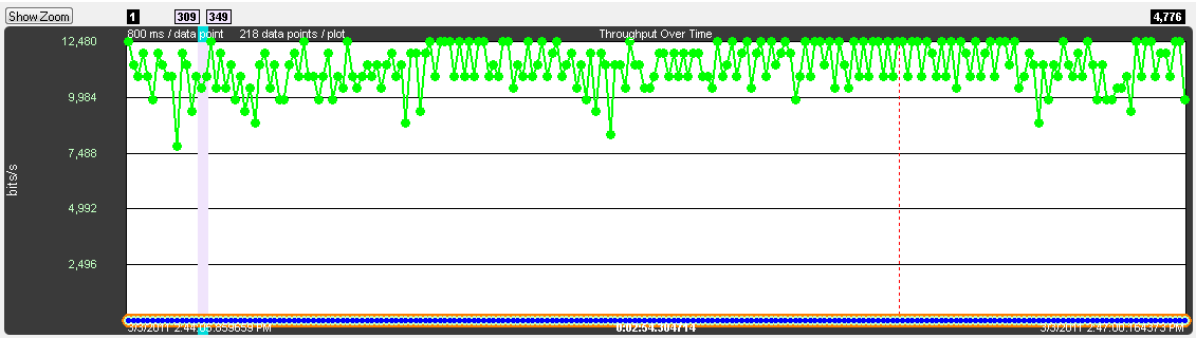


Figure 4.63 - A negative discontinuity.

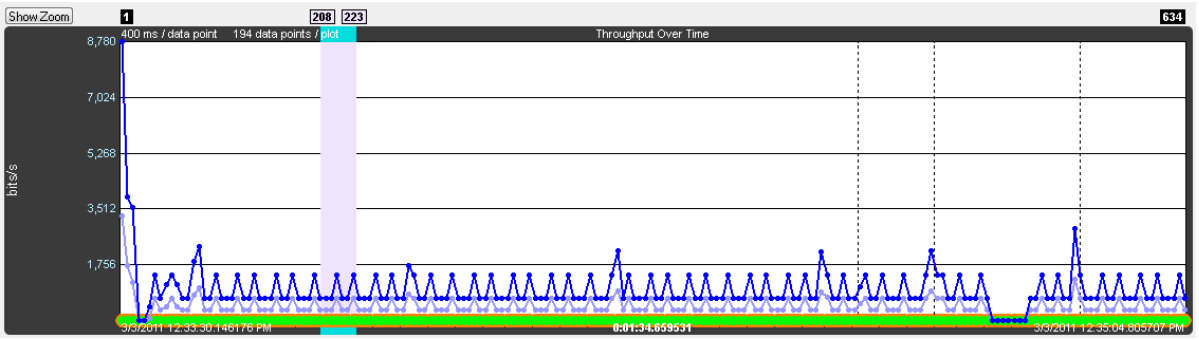


Figure 4.64 - Three positive discontinuities.

4.4.4.14 Viewport

The viewport is the purple rectangle in the **Throughput Graph**. It indicates a specific starting time, ending time, and resulting duration, and is precisely the time range used by the **Timeline**. The packet range that occurs within this time range is shown above the sides of the viewport.

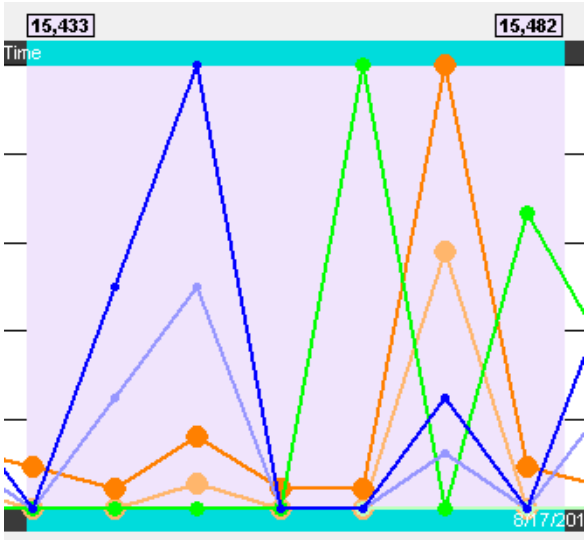


Figure 4.65 - **Throughput Graph** Viewport

The viewport is moved by dragging it or by clicking on the desired location in the **Throughput Graph** (the viewport will be centered at the click point).

The viewport is sized by dragging one of its sides or by using one of the other zooming techniques. See the Zooming subsection in the **Timeline** section for a complete list.

4.4.4.15 Swap button

The **Throughput Graph** and **Timeline** can be made to trade positions by clicking the **Swap** button.

Clicking the Swap

button swaps the positions of the **Throughput Graph**s and the **Timeline**s.

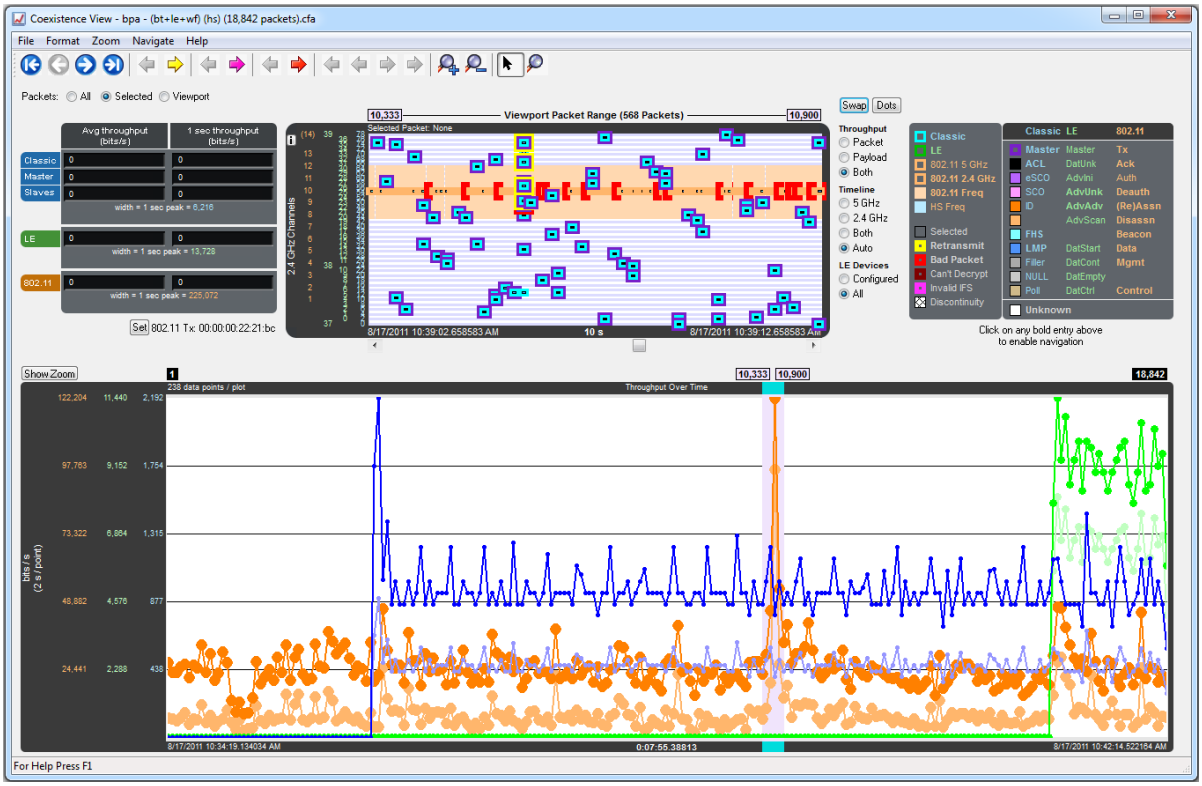


Figure 4.66 - Small Timeline and large Throughput Graph after pressing the Swap button.

4.4.4.16 Dots button

The dots on the data points can be toggled on and off by clicking the **Dots** Dots button. Dots are different sizes for each technology so that they reveal overlapping data points which otherwise wouldn't be visible. A tooltip can be displayed for each dot.

Dots can be removed for greater visibility of the plots when data points are crowded together.

Figure 4.67 - Dots Toggled On and Off

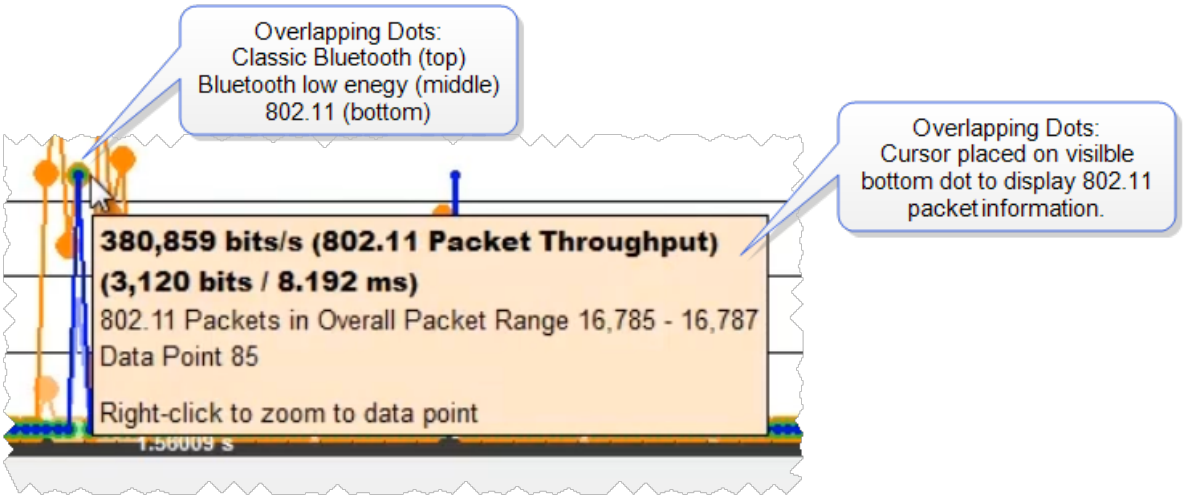

Overlapping Dots:
Classic Bluetooth (top)
Bluetooth low enegy (middle)
802.11 (bottom)
Overlapping Dots:
Cursor placed on visilble
bottom dot to display 802.11
packet information.
380,859 bits/s (802.11 Packet Throughput)
(3,120 bits / 8.192 ms)
802.11 Packets in Overall Packet Range 16,785 - 16,787
Data Point 85
Right-click to zoom to data point

Figure 4.68 - Overlapping **Dots** Information Display

4.4.4.17 Zoomed Throughput Graph

Clicking the **Show Zoom** button Show Zoom displays the **Zoomed Throughput Graph** above the **Throughput Graph**. The **Zoomed Throughput Graph** shows the details of the throughput in the time range covered by the viewport in the **Throughput Graph**. Both the **Zoomed Throughput Graph** and the **Timelines** are synchronized with the **Throughput Graph**'s viewport. The viewport is sized by dragging one of its sides or by using one of the other zooming techniques listed in the Zooming subsection in the **Timelines** section.

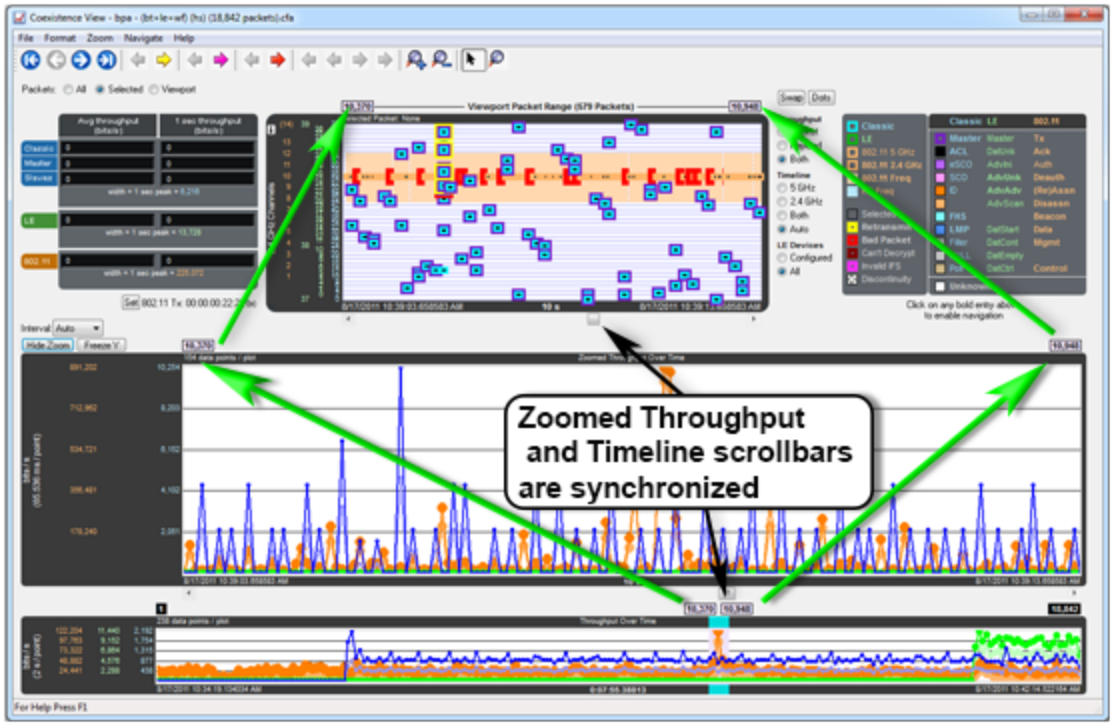


Figure 4.69 - Synchronized Zoomed Throughput Graph and View Port

The largest value in each technology in the **Zoomed Throughput Graph** is snapped to the top of the graph. This makes the graph easier to read by using all of the available space, but because the y-axis scales can change it can make it difficult to compare different time ranges or durations. Clicking the **Freeze Y** Freeze Y button freezes the y-axis scales and makes it possible to compare all time ranges and durations (the name of the button changes to **Unfreeze Y** and a **Y Scales Frozen** indicator appears to the right of the title. Clicking the **Unfreeze Y** Unfreeze Y button unfreezes the y-axis scales.

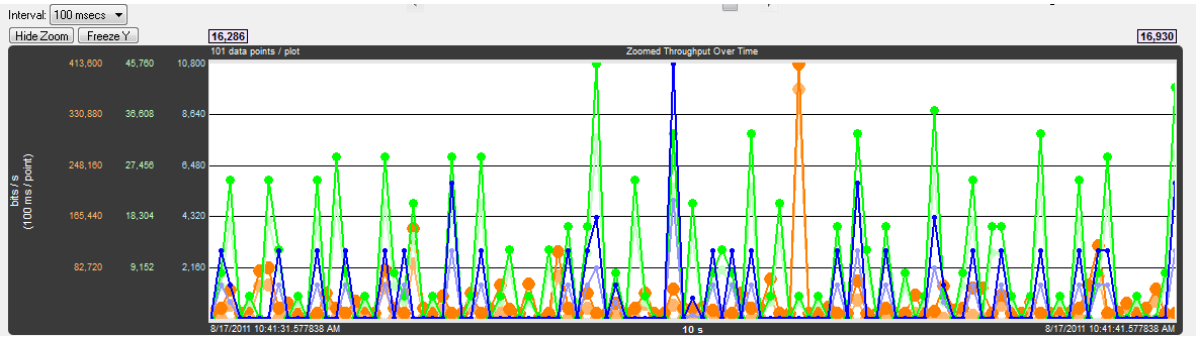


Figure 4.70 - **Zoomed Throughput Graph**- Largest Value Snaps to Top

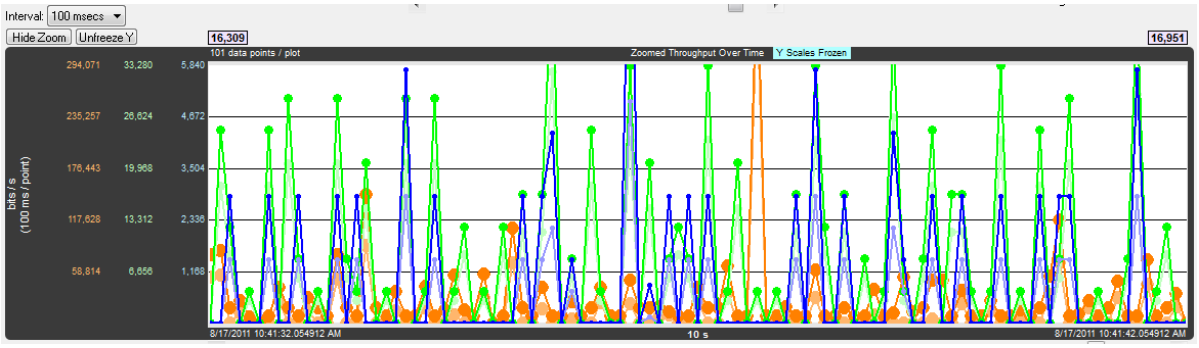
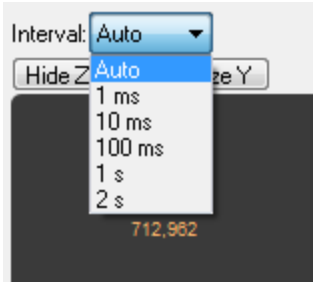


Figure 4.71 - **Zoomed Throughput Graph** - **Freeze Y** keeps the y-axis constant

Interval Menu



The **Interval** drop-down menu is used to set the duration of each data point in the Zoomed Throughput graph. The default setting is **Auto** that sets the data point interval automatically depending on the zoom level. The other menu selections provide the ability to select a fixed data point interval. Selecting from a larger to a smaller interval will display more data points. Should the number of data points exceed 30,000, no data is displayed and a warning will appear in the graph area.

4.4.4.18 Zoom Cursor

Selecting the **Zoom Cursor** button changes the cursor to the zoom cursor. The zoom cursor is controlled by the mouse wheel and zooms the viewport and thus the Timelines and the Zoomed Throughput Graph. The zoom cursor appears everywhere except the **Throughput Graph**, which is not zoomable, in which case the scroll cursor is shown. When the zoom cursor is in the **Timelines** or **Zoomed Throughput Graph** zooming occurs around the point in time where the zoom cursor is positioned. When the zoom cursor is outside the **Timelines** and the **Zoomed Throughput Graph** the left edge of those displays is the zoom point.

4.4.4.19 Comparison with the *Bluetooth* Timeline's Throughput Graph

The **Throughput Graph**s for Classic *Bluetooth* in the **Coexistence View** and the *Bluetooth***Timeline** can look quite different even though they are plotting the same data. The reason is that the **Coexistence View** uses timestamps while the *Bluetooth***Timeline** uses *Bluetooth* clocks, and they do not always match up exactly. This mismatch can result in the data for a particular packet being included in different intervals in the two **Throughput Graph**s, and can have a significant impact on the shapes of the two respective graphs. This can also result in the total duration of the two **Throughput Graph**s being different.

Another factor that can affect total duration is that the *Bluetooth***Timeline**'s **Throughput Graph** stops at the last Classic *Bluetooth* packet while the **Coexistence View**'s **Throughput Graph** stops at the last packet regardless of technology.

4.4.4.20 Coexistence View - Set Button

The **Set** button is used to specify the 802.11 source address, where any packet with that source address is considered a Tx packet and is shown with a purple border in the timelines.

All source MAC addresses that have been seen during this session are listed in the dialog that appears when the **Set** button is clicked. Also listed is the last source MAC address that was set in the dialog in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.

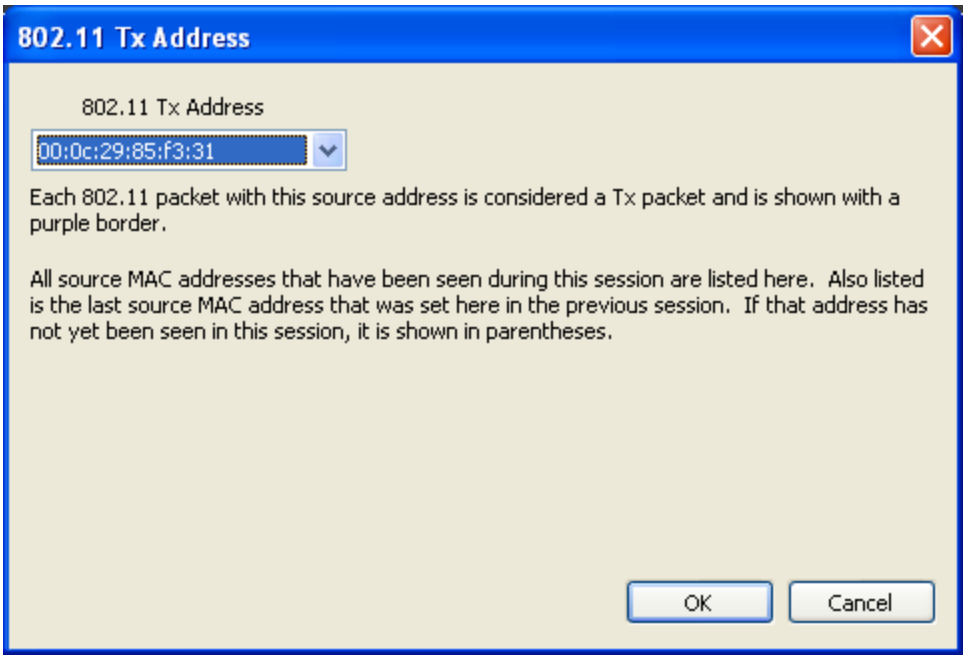

802.11 Tx Address
802.11 Tx Address
00:0c:29:85:f3:31
Each 802.11 packet with this source address is considered a Tx packet and is shown with a purple border.
All source MAC addresses that have been seen during this session are listed here. Also listed is the last source MAC address that was set here in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.
OK
Cancel

Figure 4.72 - 802.11 Source Address Dialog

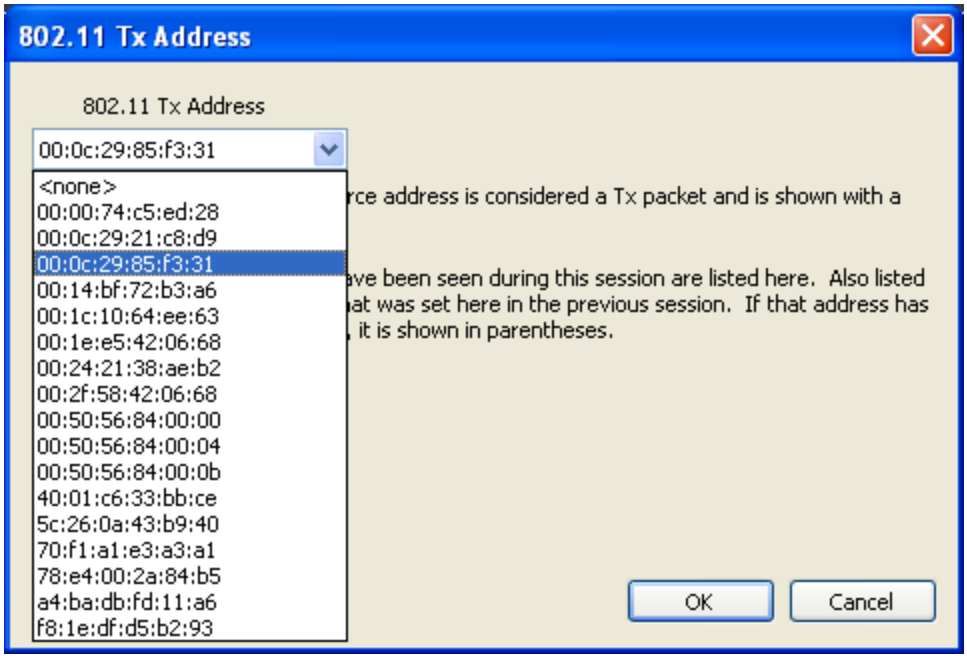
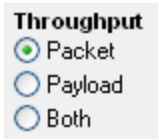


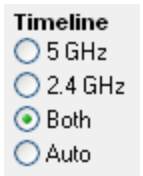
Figure 4.73 - 802.11 Source Address Drop Down Selector

4.4.4.21 Coexistence View - Throughput Radio Buttons



The radio buttons in the Throughput group specify whether to show packet and/or payload lines in the Throughput Graph, and also whether to show packet or payload throughput in the throughput indicators (if the Both radio button is selected, packet throughput is shown in the throughput indicators).

4.4.4.22 Coexistence View - Timeline Radio Buttons



The radio buttons in the **Timeline** group specify timeline visibility. The first three buttons specify whether to show one or both timelines, while the **Auto** button shows only timelines which have had packets at some point during this session. If no packets have been received at all and the **Auto** button is selected the 2.4 GHz timeline is shown.

4.4.4.23 Coexistence View – low energy Devices Radio Buttons

The radio buttons in the **LE Devices** group (where "LE" means Bluetooth® low energy) specify both visibility and inclusion in throughput calculations of *Bluetooth* low energy packets. The **All** radio button shows and uses all *Bluetooth* low energy packets. The Configured radio button shows and uses only *Bluetooth* low energy packets which come from a configured device.

4.4.4.24 Coexistence View – Legend

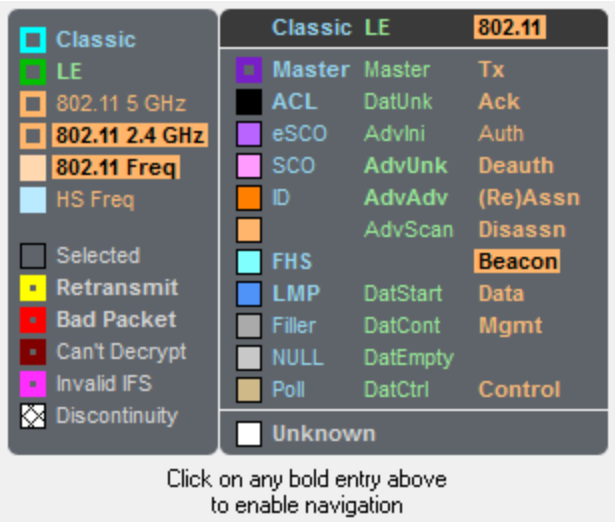


Figure 4.74 - Coexistence View Legend

The legend describes the color-coding used by packets in the timelines. Selecting a packet in a timeline highlights the applicable entries in the legend. An entry is bold if any such packets currently exist. Clicking on a bold entry enables the black legend navigation arrows in the toolbar for that entry.

4.4.4.25 Coexistence View – Timelines

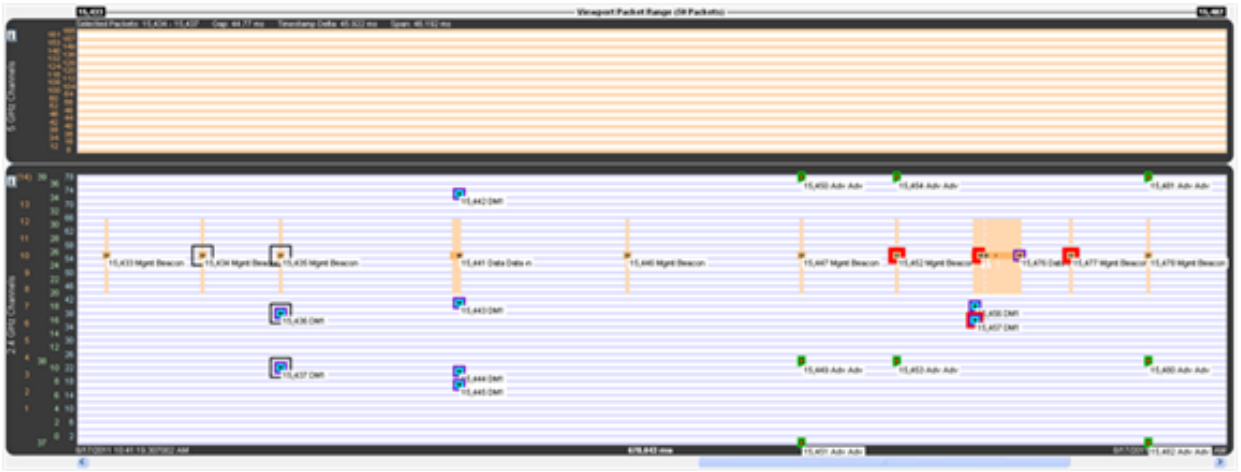


Figure 4.75 - Coexistence View Timelines

The **Timelines** show Classic Bluetooth® , *Bluetooth* low energy, and 802.11 packets by channel and time.

4.4.4.26 Packet information

Packet information is provided in various ways as described below.

Packets are color-coded to indicate attribute (Retransmit, Bad Packet, Can't Decrypt, or Invalid IFS), master/Tx, technology (Classic Bluetooth® , *Bluetooth* low energy, or 802.11), and category/type.

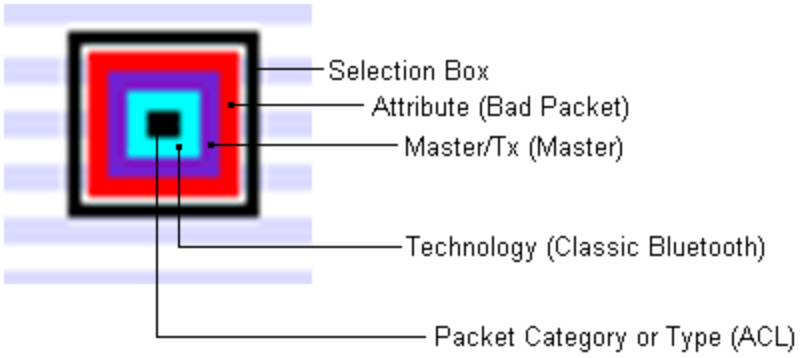


Figure 4.76 - Each packet is color-coded

The innermost box (which indicates packet category/type) is the packet proper in that its vertical position indicates the channel, its length indicates the packet's duration in the air, its left edge indicates the start time, and its right edge indicates the end time.

The height of Classic *Bluetooth* and *Bluetooth* low energy packets indicates their frequency range (1 MHz and 2 MHz respectively). Since 802.11 channels are so wide (22 MHz), 802.11 packets are drawn with an arbitrary 1 MHz height and centered within a separate frequency range box which indicates the actual frequency range.

Selecting a packet by clicking on it draws a selection box around it (as shown above) and highlights the applicable entries in the legend.

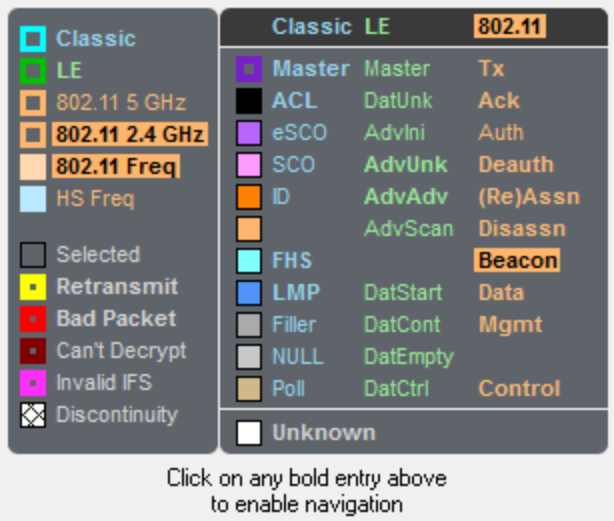


Figure 4.77 - Highlighted entries in the legend for a selected packet.

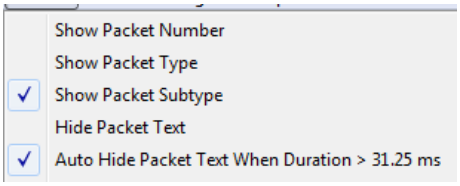
Summary information for a selected packet is displayed in the timeline header.

Selected Packet: 15,457 Timestamp: 8/17/2011 10:41:19.835783 AM Technology: Classic Type: DM1 Bluetooth Clock: 0x0113e610 Payload Len: 9 bytes

Figure 4.78 - **Timeline** header for a single selected packet.

When multiple packets are selected (by dragging the mouse with the left button held down, clicking one packet and shift-clicking another, or clicking one packet and pressing shift-arrow), the header shows **Gap** (duration between the first and last selected packets), **Timestamp Delta** (difference between the timestamps, which are at the beginning of each packet), and **Span** (duration from the beginning of the first selected packet to the end of the last selected packet).

Figure 4.79 - **Timeline** header for multiple selected packets



Text can be displayed at each packet by selecting **Show Packet Number**, **Show Packet Type**, and **Show Packet Subtype** from the **Format** menu.

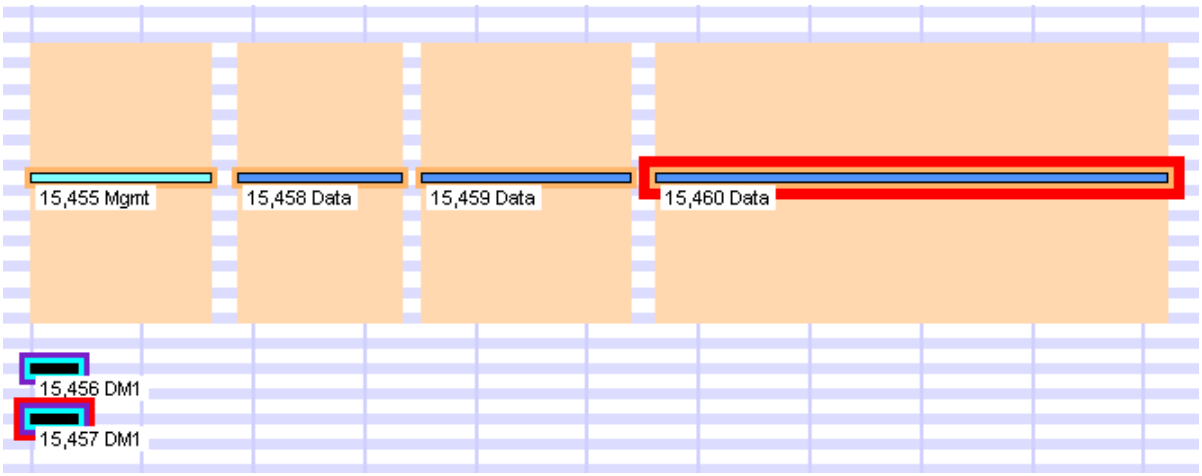


Figure 4.80 - Descriptive text on timeline packets.

Placing the mouse pointer on a packet displays a tooltip (color-coded by technology) that gives detailed information.

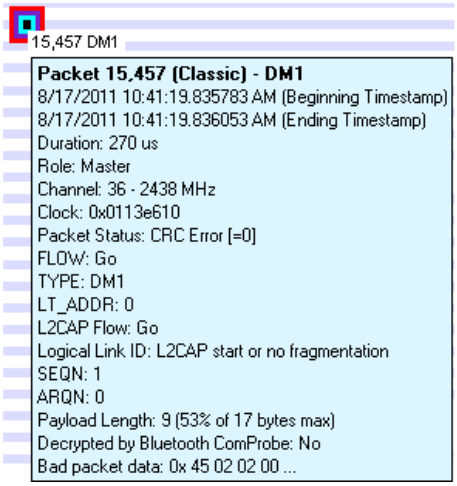

15,457 DM1
Packet 15,457 (Classic) - DM1
8/17/2011 10:41:19.835783 AM (Beginning Timestamp)
8/17/2011 10:41:19.836053 AM (Ending Timestamp)
Duration: 270 us
Role: Master
Channel: 36 - 2438 MHz
Clock: 0x0113e610
Packet Status: CRC Error [=0]
FLOW: Go
TYPE: DM1
LT_ADDR: 0
L2CAP Flow: Go
Logical Link ID: L2CAP start or no fragmentation
SEQN: 1
ARQN: 0
Payload Length: 9 (53% of 17 bytes max)
Decrypted by Bluetooth ComProbe: No
Bad packet data: 0x 45 02 02 00 ...

Figure 4.81 - A tool tip for a Classic *Bluetooth* packet.

4.4.4.27 Relocating the tool tip

You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. In the **Format** menu select **Show Tooltips in Upper-Left Corner of Screen**, and any time you mouse-over a packet the tool tip will appear anchored in the upper-left corner of the computer screen. To return to viewing the tool tip adjacent to the packets deselect the tool tip format option in the menu.

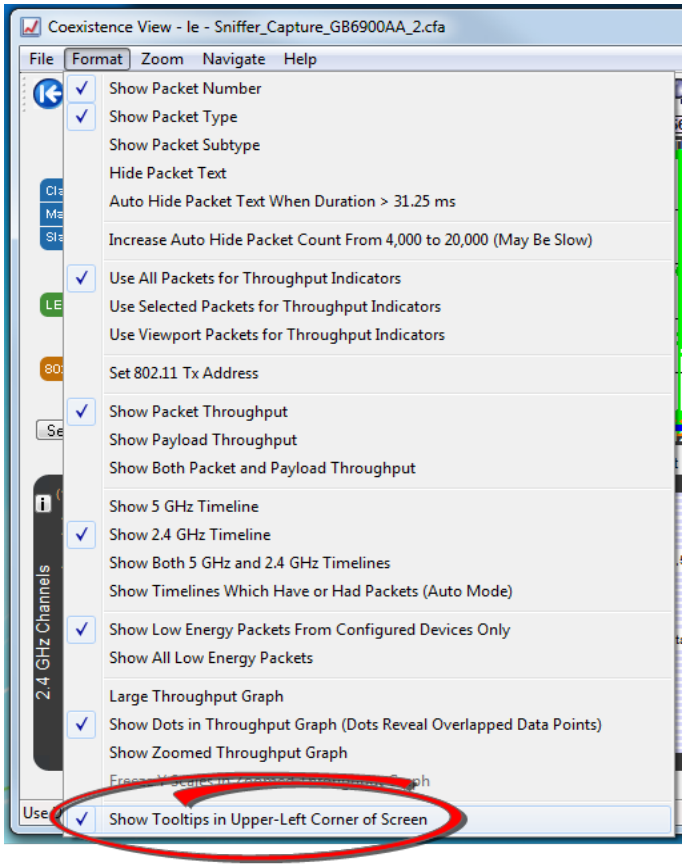

Coexistence View - le - Sniffer_Capture_GB6900AA_2.cfa
File
Format
Zoom
Navigate
Help
Show Packet Number
Show Packet Type
Show Packet Subtype
Hide Packet Text
Auto Hide Packet Text When Duration > 31.25 ms
Increase Auto Hide Packet Count From 4,000 to 20,000 (May Be Slow)
Use All Packets for Throughput Indicators
Use Selected Packets for Throughput Indicators
Use Viewport Packets for Throughput Indicators
Set 802.11 Tx Address
Show Packet Throughput
Show Payload Throughput
Show Both Packet and Payload Throughput
Show 5 GHz Timeline
Show 2.4 GHz Timeline
Show Both 5 GHz and 2.4 GHz Timelines
Show Timelines Which Have or Had Packets (Auto Mode)
Show Low Energy Packets From Configured Devices Only
Show All Low Energy Packets
Large Throughput Graph
Show Dots in Throughput Graph (Dots Reveal Overlapped Data Points)
Show Zoomed Throughput Graph
Show Tooltips in Upper-Left Corner of Screen
2.4 GHz Channels

Figure 4.82 - Coexistence View Format Menu - Show Tooltips on Computer Screen

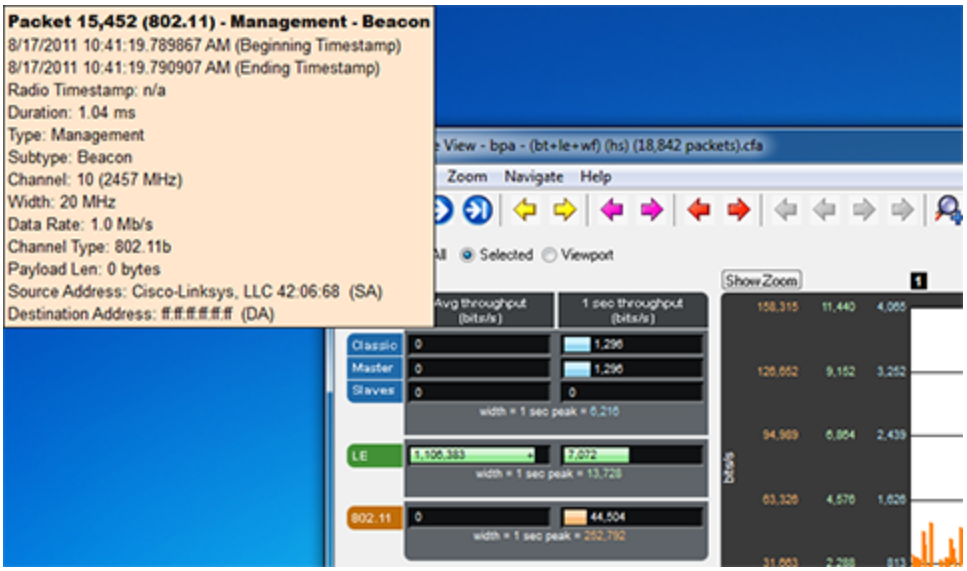


Figure 4.83 - Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen

4.4.4.28 The two Timelines

There are two **Timelines** available for viewing, one for the 5 GHz range and one for the 2.4 GHz range. Classic *Bluetooth* and *Bluetooth* low energy occur only in the 2.4 GHz range. 802.11 can occur in both.

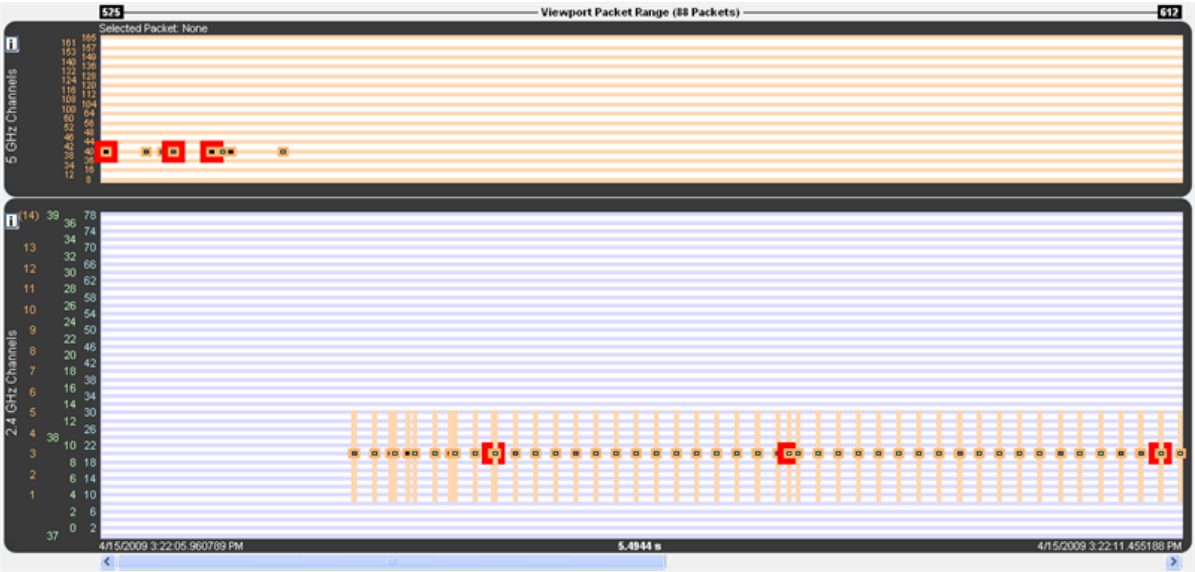


Figure 4.84 - 5 GHz and 2.4 GHz 802.11 packets

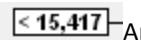
The y-axis labels show the channels for each technology and are color-coded: Blue = Classic *Bluetooth*, Green = *Bluetooth* low energy, Orange = 802.11.

The 5 GHz timeline has only 802.11 channel labels, and the rows alternate orange and white, one row per channel.

The 2.4 GHz timeline has labels for all three technologies. The rows alternate blue and white, one row per Classic *Bluetooth* channel. The labels going left-to-right are 802.11 channels, *Bluetooth* low energy advertising channels, *Bluetooth* low energy regular channels, and Classic *Bluetooth* channels.

The **Viewport Packet Range** above the timelines shows the packet range and packet count of packets that would be visible if both timelines were shown (i.e. hiding one of the timelines doesn't change the packet range or count). This packet range matches the packet range shown above the viewport in the Throughput Graph, as it must since the viewport defines the time range used by the timelines. When no packets are in the time range, each of the two packet numbers is drawn with an arrow to indicate the next packet in each direction and can be clicked on to navigate to that packet (the packet number changes color when the mouse pointer is placed on it in this case).

An arrow points to the next packet when no packets are in the time range.



An arrowed packet number changes color when the mouse pointer is on it. Clicking navigates to that packet.

The header shows information for packets that are selected.

The footer shows the beginning/ending timestamps and visible duration of the timelines.

The 'i' buttons bring up channel information windows, which describe channel details for each technology. They make for interesting reading.

802.11 5 GHz

Only channels with a base value of 5 GHz and spacings of either 20 or 40 MHz are shown here. Due to space limitations, each channel is drawn with fixed spacing instead of being spaced relative to its distance from other channels as is done with 2.4 GHz channels (with the exception of 802.11 channel 14).

Figure 4.85 - 5 GHz information window

Bluetooth Classic

There are 79 Classic channels. Each channel is 1 MHz wide and has the indicated center frequency. Channels do not overlap.

0 = 2402 MHz	10 = 2412 MHz	20 = 2422 MHz	30 = 2432 MHz	40 = 2442 MHz	50 = 2452 MHz	60 = 2462 MHz	70 = 2472 MHz
1 = 2403 MHz	11 = 2413 MHz	21 = 2423 MHz	31 = 2433 MHz	41 = 2443 MHz	51 = 2453 MHz	61 = 2463 MHz	71 = 2473 MHz
2 = 2404 MHz	12 = 2414 MHz	22 = 2424 MHz	32 = 2434 MHz	42 = 2444 MHz	52 = 2454 MHz	62 = 2464 MHz	72 = 2474 MHz
3 = 2405 MHz	13 = 2415 MHz	23 = 2425 MHz	33 = 2435 MHz	43 = 2445 MHz	53 = 2455 MHz	63 = 2465 MHz	73 = 2475 MHz
4 = 2406 MHz	14 = 2416 MHz	24 = 2426 MHz	34 = 2436 MHz	44 = 2446 MHz	54 = 2456 MHz	64 = 2466 MHz	74 = 2476 MHz
5 = 2407 MHz	15 = 2417 MHz	25 = 2427 MHz	35 = 2437 MHz	45 = 2447 MHz	55 = 2457 MHz	65 = 2467 MHz	75 = 2477 MHz
6 = 2408 MHz	16 = 2418 MHz	26 = 2428 MHz	36 = 2438 MHz	46 = 2448 MHz	56 = 2458 MHz	66 = 2468 MHz	76 = 2478 MHz
7 = 2409 MHz	17 = 2419 MHz	27 = 2429 MHz	37 = 2439 MHz	47 = 2449 MHz	57 = 2459 MHz	67 = 2469 MHz	77 = 2479 MHz
8 = 2410 MHz	18 = 2420 MHz	28 = 2430 MHz	38 = 2440 MHz	48 = 2450 MHz	58 = 2460 MHz	68 = 2470 MHz	78 = 2480 MHz
9 = 2411 MHz	19 = 2421 MHz	29 = 2431 MHz	39 = 2441 MHz	49 = 2451 MHz	59 = 2461 MHz	69 = 2471 MHz	

The row labels are placed at the center frequency of each channel.

Bluetooth low energy (LE)

There are 40 LE channels. Each channel is 2 MHz wide and has the indicated center frequency. Channels do not overlap.
Channels 0 through 36 are Data channels. Channels 37 through 39 are Advertising channels.

37 = 2402 MHz	4 = 2412 MHz	9 = 2422 MHz	13 = 2432 MHz	18 = 2442 MHz	23 = 2452 MHz	28 = 2462 MHz	33 = 2472 MHz
0 = 2404 MHz	5 = 2414 MHz	10 = 2424 MHz	14 = 2434 MHz	19 = 2444 MHz	24 = 2454 MHz	29 = 2464 MHz	34 = 2474 MHz
1 = 2406 MHz	6 = 2416 MHz	38 = 2426 MHz	15 = 2436 MHz	20 = 2446 MHz	25 = 2456 MHz	30 = 2466 MHz	35 = 2476 MHz
2 = 2408 MHz	7 = 2418 MHz	11 = 2428 MHz	16 = 2438 MHz	21 = 2448 MHz	26 = 2458 MHz	31 = 2468 MHz	36 = 2478 MHz
3 = 2410 MHz	8 = 2420 MHz	12 = 2430 MHz	17 = 2440 MHz	22 = 2450 MHz	27 = 2460 MHz	32 = 2470 MHz	39 = 2480 MHz

The row labels are placed at the center frequency of each channel.

802.11 2.4 GHz

In the 802.11 2.4 GHz frequency range there are 11 channels in the USA, 13 in Europe, and 14 in Japan. Each channel is 22 MHz wide. Channels overlap.
There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.

1 = 2401-2423 MHz	(centered at 2412 MHz)	(USA, Europe, Japan)	8 = 2436-2458 MHz	(centered at 2447 MHz)	(USA, Europe, Japan)	
2 = 2406-2428 MHz	(centered at 2417 MHz)	(USA, Europe, Japan)	9 = 2441-2463 MHz	(centered at 2452 MHz)	(USA, Europe, Japan)	
3 = 2411-2433 MHz	(centered at 2422 MHz)	(USA, Europe, Japan)	10 = 2446-2468 MHz	(centered at 2457 MHz)	(USA, Europe, Japan)	
4 = 2416-2438 MHz	(centered at 2427 MHz)	(USA, Europe, Japan)	11 = 2451-2473 MHz	(centered at 2462 MHz)	(USA, Europe, Japan)	
5 = 2421-2443 MHz	(centered at 2432 MHz)	(USA, Europe, Japan)	12 = 2456-2478 MHz	(centered at 2467 MHz)	(Europe, Japan)	
6 = 2426-2448 MHz	(centered at 2437 MHz)	(USA, Europe, Japan)	13 = 2461-2483 MHz	(centered at 2472 MHz)	(Europe, Japan)	
7 = 2431-2453 MHz	(centered at 2442 MHz)	(USA, Europe, Japan)	14 = 2473-2495 MHz	(centered at 2484 MHz)	(Japan)	

The row labels for 802.11 channels 1-13 are placed at the center frequency of each channel.
The row label for 802.11 channel 14 is in parentheses because that channel's center frequency is above the top of the graph.

Figure 4.86 - 2.4 GHz information windows

4.4.4.29 *Bluetooth* slot markers

When zoomed in far enough *Bluetooth* slot markers appear in the 2.4 GHz timeline. A *Bluetooth* slot is 625 µs wide.

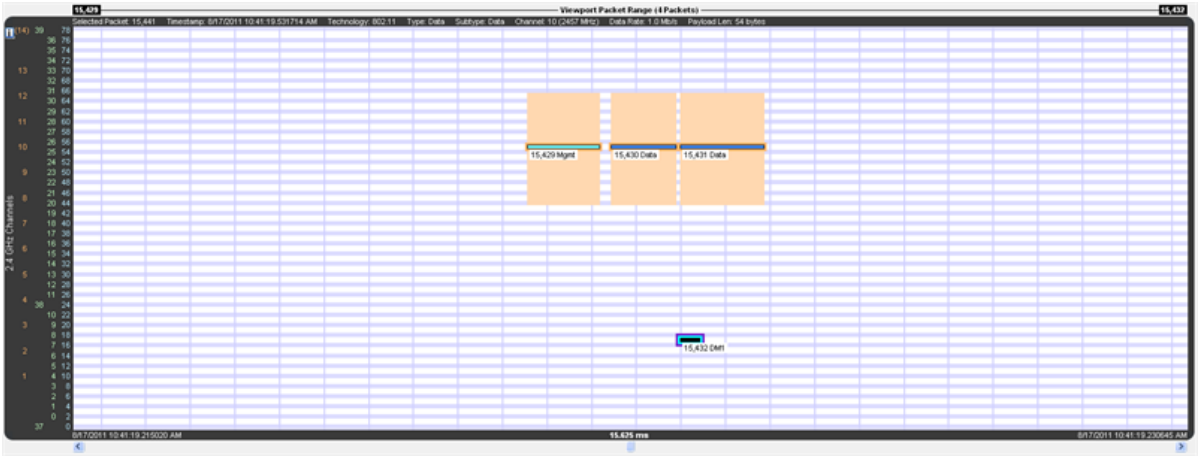


Figure 4.87 - Vertical blue lines are *Bluetooth* slot markers

4.4.4.30 Zooming

There are various ways to zoom:

1. Drag one of the sides of the **Throughput Graph** viewport.
2. Select a zoom preset from the **Zoom** or right-click menus.
3. Select the **Zoom In** or **Zoom Out** button or menu item.
4. Turn the mouse wheel in the **Timelines** or the **Zoomed Throughput Graph** while the zoom cursor is selected. The action is the same as selecting the **Zoom In** and **Zoom Out** buttons and menu items except that the time point at the mouse pointer is kept in place if possible.
5. Select the **Zoom to Data Point Packet Range** menu item, which zooms to the packet range shown in the most recently displayed tool tip.
6. Select the **Zoom to Selected Packet Range** menu item, which zooms to the selected packet range as indicated in the **Selected Packets** text in the timeline header.
7. Select the **Custom Zoom** menu item. This is the zoom level from the most recent drag of a viewport side, selection of **Zoom to Data Point Packet Range**, or selection of **Zoom to Selected Packet**.

The zoom buttons and tools step through the zoom presets and custom zoom, where the custom zoom is logically inserted in value order into the zoom preset list for this purpose.

4.4.4.31 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s (this value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s). A discontinuity is drawn as a vertical cross-hatched area one *Bluetooth* slot (625 µs) in width. A discontinuity for a timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

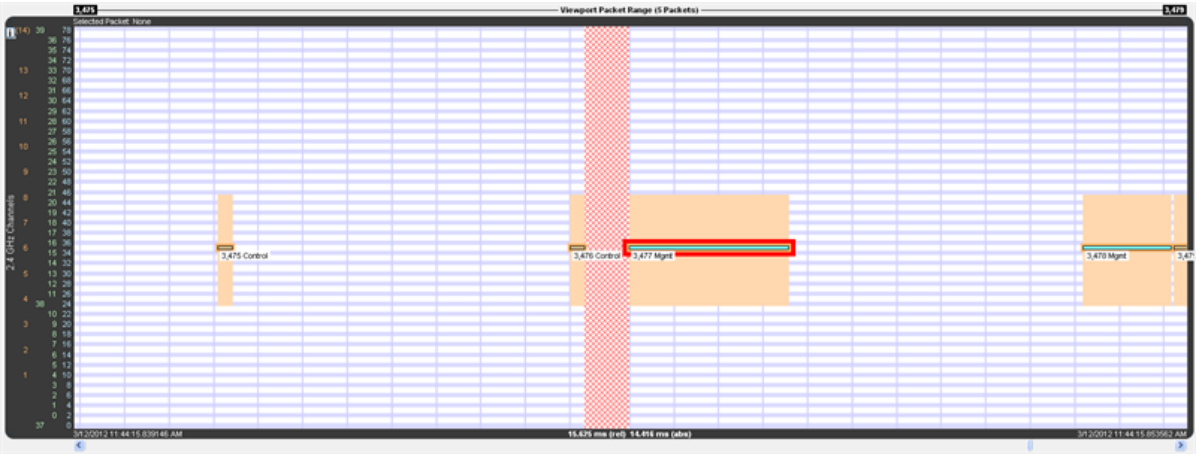


Figure 4.88 - A negative discontinuity

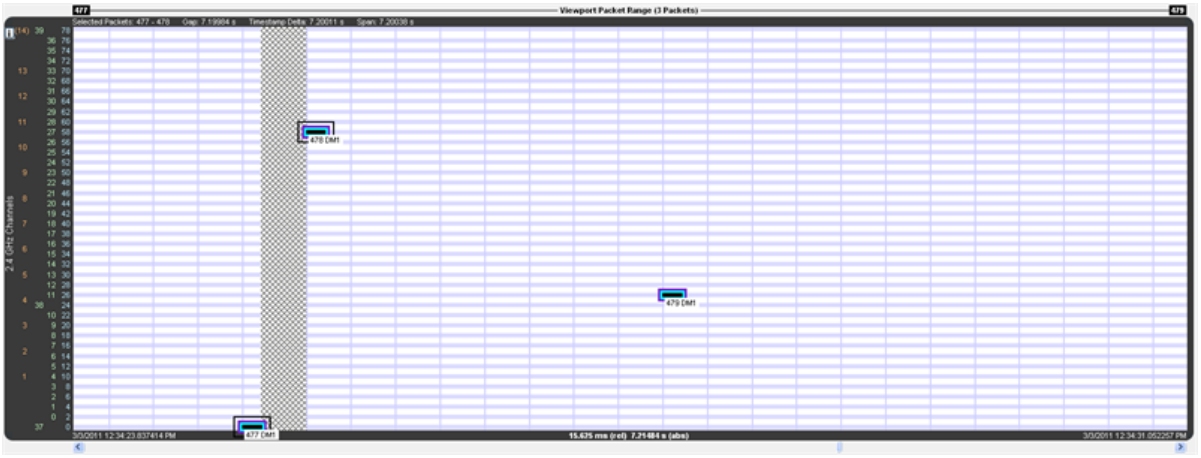


Figure 4.89 - A positive discontinuity

When there are one or more discontinuities the actual time encompassed by the visible timeline differs from the zoom level duration that would apply in the absence of any discontinuities. The actual time, referred to as absolute time, is shown followed by "(abs)". The zoom level duration, referred to as relative time, is shown followed by "(rel)". When there are no discontinuities, relative and absolute time are the same and a single value is shown.

Figure 4.90 - Timeline header with discontinuity

Figure 4.91 - Timeline duration footer with discontinuity

For example, the timeline above has a zoom level duration of 15.625 ms (the relative time shown in the footer). But the discontinuity graphic consumes the width of a *Bluetooth* slot (625 µs), and that area is 7.19984 s of absolute time as shown by the Gap value in the header. So the absolute time is 7.21484 s:

Zoom level duration – *Bluetooth* slot duration + Gap duration =

15.625 ms - 625 µs + 7.19984 s =

0.015625 s – 0.000625 s + 7.199840 s =

0.015000 s + 7.199840 s =

7.214840 s =

7.21484 s

4.4.4.32 High-Speed *Bluetooth*

High-speed *Bluetooth* packets, where *Bluetooth* content hitches a ride on 802.11 packets, have a blue frequency range box instead of orange as with regular 802.11 packets (both are shown below), and the tool tip has two colors, orange for 802.11 layers and blue for *Bluetooth* layers.

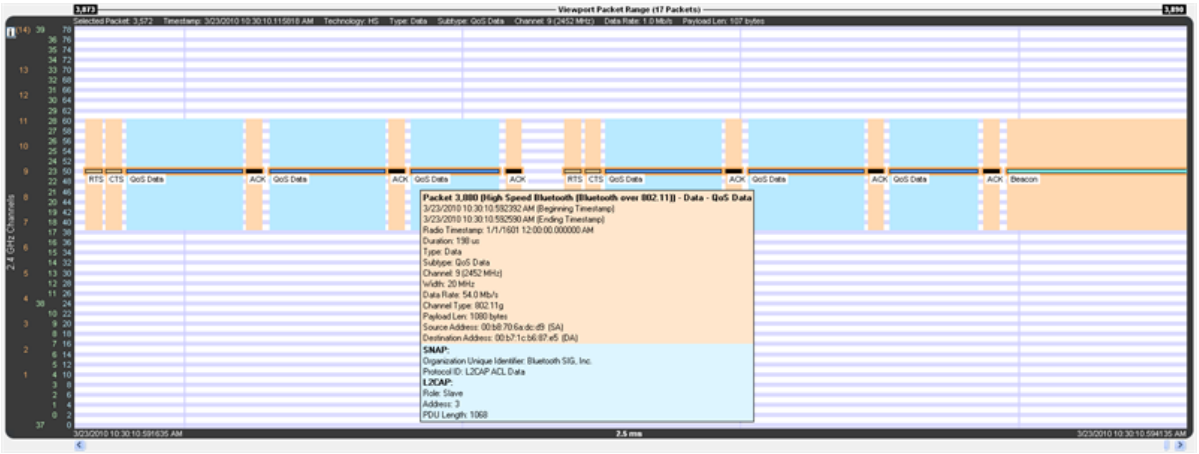


Figure 4.92 - High-speed *Bluetooth* packets have a blue frequency box and a two-tone tool tip

4.4.4.33 Coexistence View - No Packets Displayed with Missing Channel Numbers

Note: This topic applies only to Classic *Bluetooth*.

Captured packets that don't contain a channel number, such as HCI and BTSnoop, will not be displayed. When no packets have a channel number the **Coexistence View Throughput Graph** and **Timelines** will display a message: "Packets without a channel number (such as HCI) won't be shown."

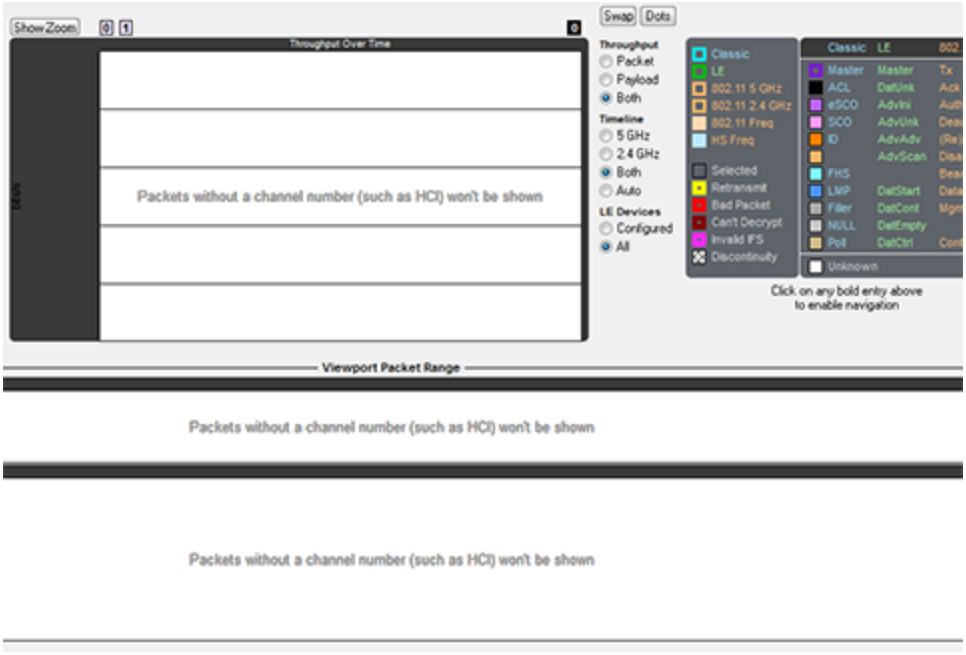


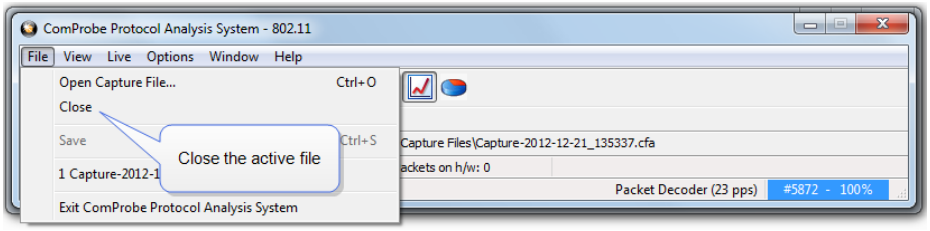
Figure 4.93 - Missing Channel Numbers Message in Timelines

4.4.4.34 High Speed Live View

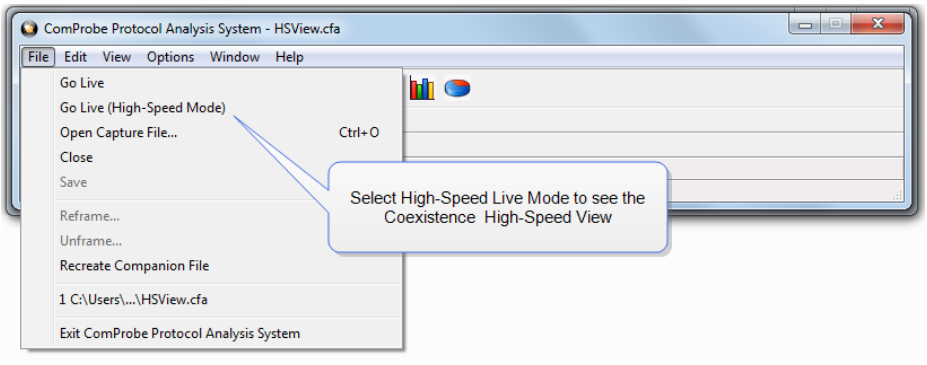
When using the ComProbe 802.11 in conjunction with other ComProbe devices, or in a stand-alone configuration, a smaller version of the standard **Coexistence View** is available. This **High Speed Live View** is essentially the **Viewport** from the standard **Coexistence View**.

When viewing **High Speed Live**, only 802.11 traffic is visible. Because Bluetooth® packets are slow they are not visible in High Speed mode.

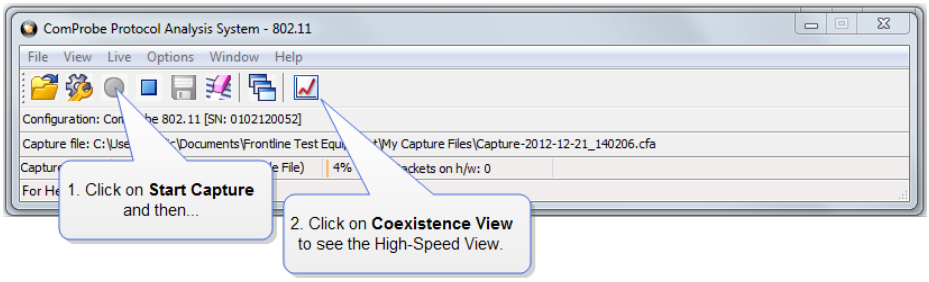
1. Click on the **Control** window **File** menu and select **Close**.



2. The **Control** window will open again. Click on the Control Window **File** menu and select **Go Live (High-Speed Mode)**



3. Click on the **Control** window **Start Capture** button to begin capturing data. Click on the **Coexistence View** button and the **High-Speed View** will appear.


ComProbe Protocol Analysis System - 802.11
File View Live Options Window Help
1. Click on Start Capture and then...
2. Click on Coexistence View to see the High-Speed View.

The Coexistence View (High Speed Live Mode) window will appear.

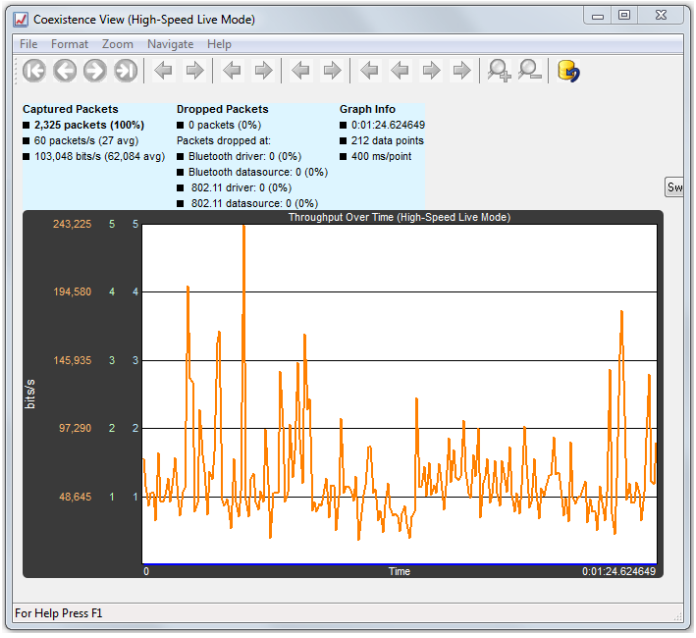


Figure 4.15 High-Speed Live Window

4.4.5 About The Message Sequence Chart (MSC)

The **Message Sequence Chart** (MSC) displays information about the messages passed between protocol layers. MSC displays a concise overview of a *Blutetooth* connection, highlighting the essential elements fo the connection. At a glance, you can see the flow of the data including role switches, connection requests, and errors. You can look at all the packets int he capture, or filter by protocol or profile. the MSC is color coded for a clear and easy view of your data.

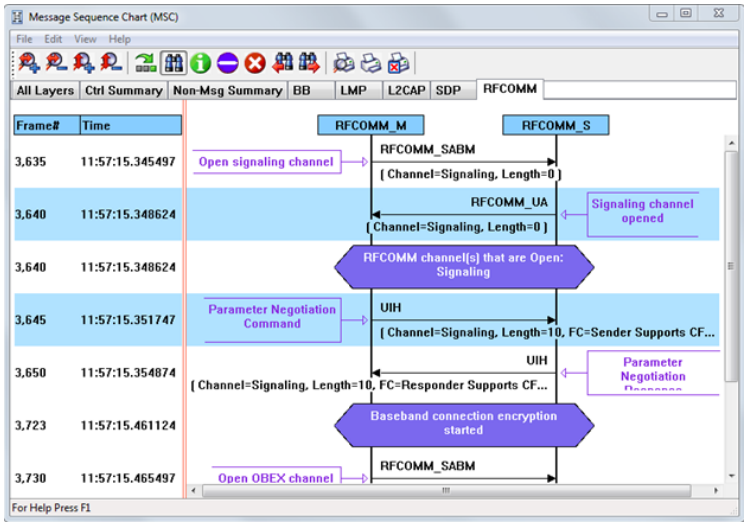


Figure 4.94 - Message Sequence Chart Window

How do I access the chart?

You access the **Message Sequence Chart** by selecting the icon or **MSC Chart** from the **View** menu from the **Control** window or **Frame Display**.

What do I see on the dialog?

At the top of the dialog you see four icons that you use to zoom in and out of the display vertically and horizontally. The same controls are available under the **View** menu.

There are three navigation icons also on the toolbar.

	This takes you to the first Information Frame.
	This takes you to first Protocol State Message.
	This takes you to the first Error Frame. Click here to learn more about this option.

If there is both Classic and low energy packets, there will be a **Classic** and **LE** tab at the top of the dialog.

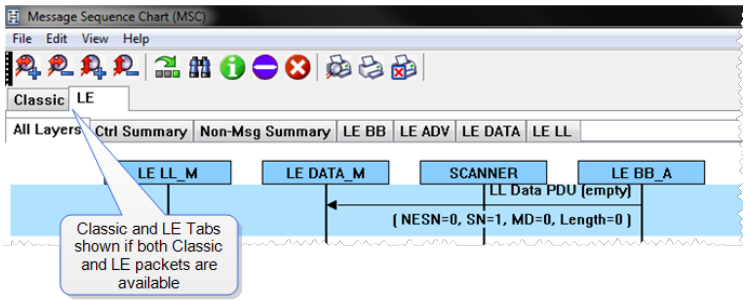
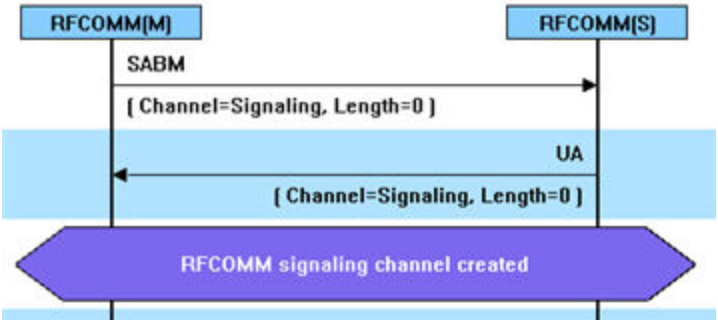

Message Sequence Chart (MSC)
File Edit View Help
Classic LE
All Layers Ctrl Summary Non-Msg Summary LE BB LE ADV LE DATA LE LL
LE LL_M
LE DATA_M
SCANNER
LE BB_A
LL Data PDU [empty]
[NESN=0, SN=1, MD=0, Length=0]
Classic and LE Tabs shown if both Classic and LE packets are available

Figure 4.95 - Classic and LE tabs

If the **Classic** tab is selected, you will see Classic protocols. If you select the **LE** tab, you will see LE Protocols. If there is only Classic or only LE, the Classic and LE tabs will not appear.

Also along the top of the dialog are a series of protocol tabs. The tabs will vary depending on the protocols.

Clicking on a tab displays the messaging between the master and slave for that protocol. For example, if you select **RFCOMM**, you will see the messaging between the **RFCOMM{M}** Master, and the **RFCOMM{S}** Slave.



The Non-Message Summary tab displays all the non-message items in the data.

The **Ctrl Summary** tab displays the signaling packets for all layers in one window in the order in which they are received.

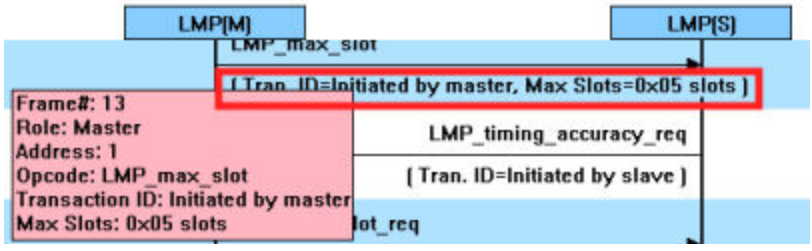
The information in the colored boxes displays general information about the messaging. The same is true for each one of the protocols.

If you want to see the all the messaging in one dialog, you select the **All Layers** tab.

When you move the mouse over the message description you see an expanded tool tip.

If you position the cursor outside of the message box, the tool tip will only display for a few seconds.

If, however, you position the cursor within the tool tip box, the message will remain until you move the cursor out of the box.



Additionally, If you right click on a message description, you will see the select Show all Layers button.

When you select **Show all Layers**, the chart will display all the messaging layers.

The **Frame#** and **Time** of the packets are displayed on the left side of the chart.

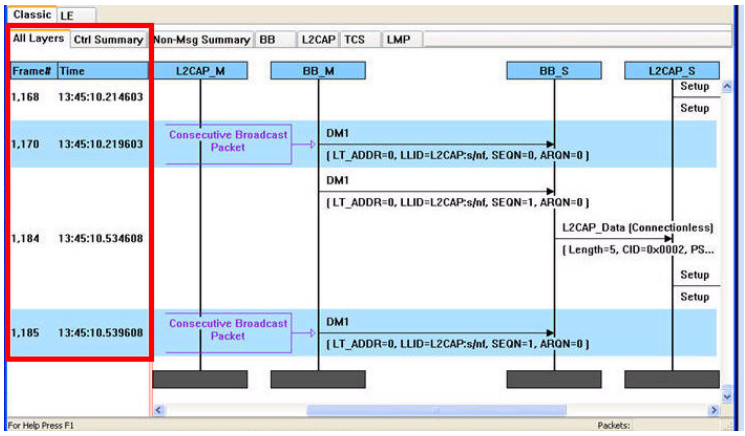


Figure 4.96 - Frame# and Time Display, inside red box.

If you click on the description of the message interaction, the corresponding information is highlighted in Frame Display.

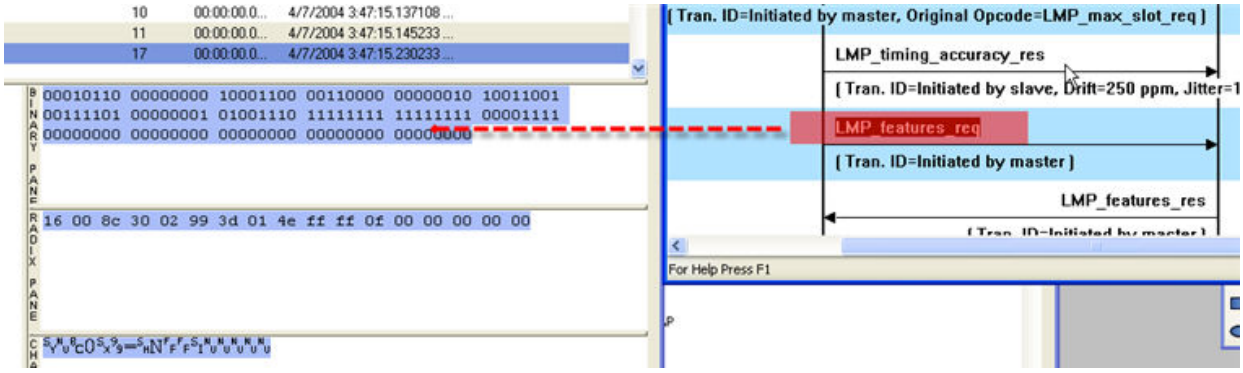


Figure 4.97 - MSC Synchronization with Frame Display

How do I navigate in the dialog?

You can use the navigation arrows at the bottom and the right side of the dialog to move vertically and horizontally. You can also click and hold while moving the pointer within dialog that brings up a directional arrow that you can use to move left/right and up/down.

Ctrl Summary tab

When you select the **Ctrl Summary tab** you will see a summary of the control and signaling frames in the order that they are received/transmitted from and to devices.

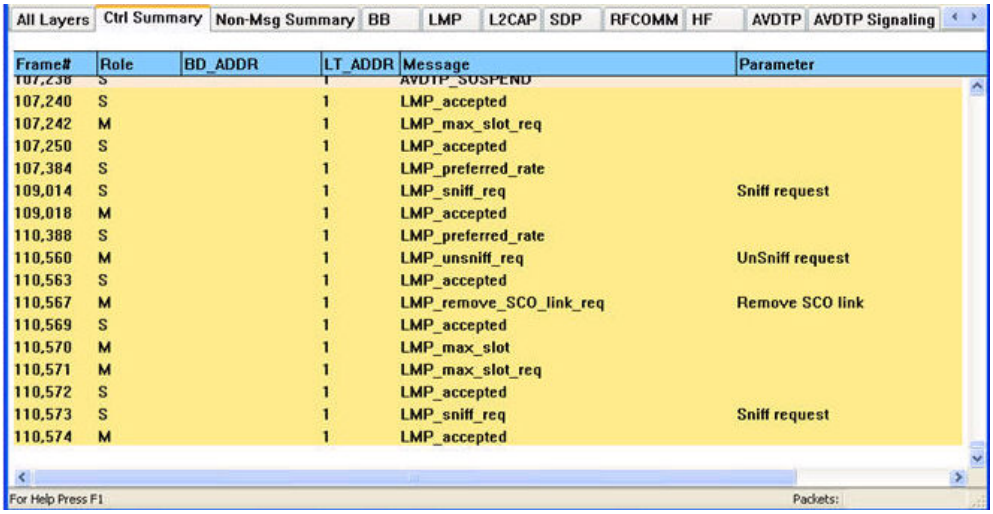


Figure 4.98 - Control and Signaling Frames Summay

The frame numbered is shown, whether the message comes from the Master or Slave, the message Address, the message itself, and the timestamp.

Additionally, the control/signaling packets for each layer are shown in a different background color.

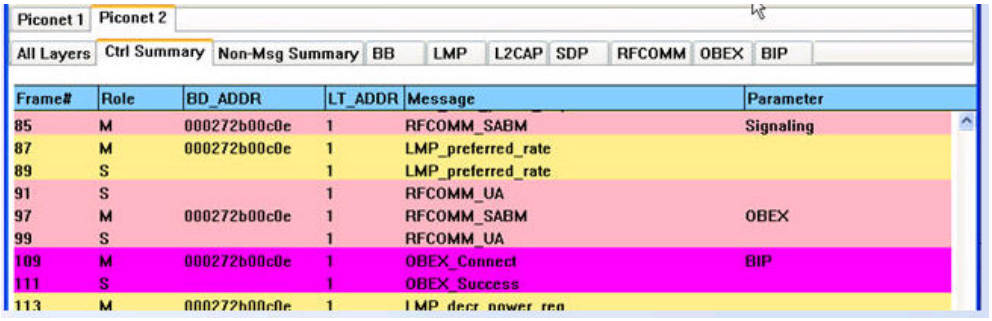


Figure 4.99 - Packet Layers Shown in Different Colors

If you right click within the **Ctrl Summary**, you can select **Show in MSC**.

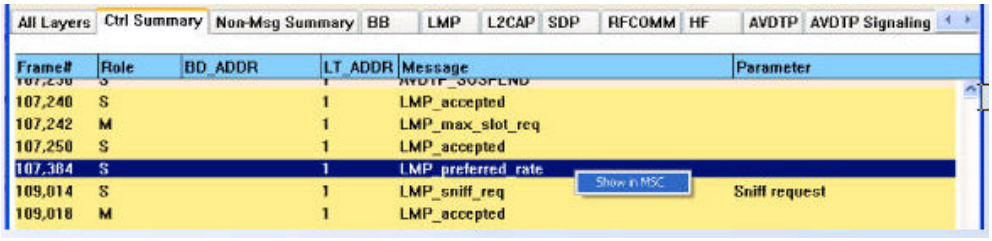


Figure 4.100 - Right-Click in Ctrl Summary to Display Show in MSC

The window then displays the same information, but in the normal MSC view.

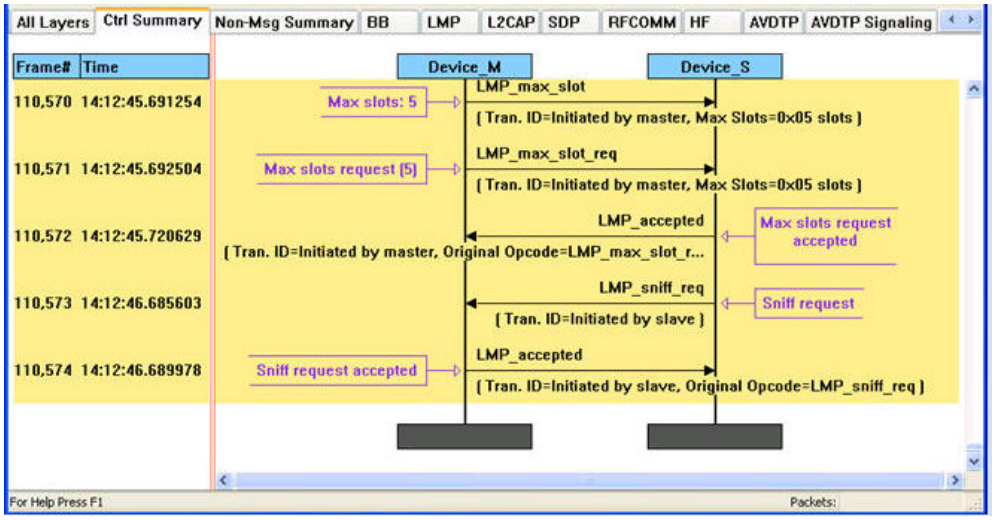


Figure 4.101 - MSC View of Selected Packet from Ctrl Summary

You can return to the text version by using a right click and selecting **Show in Text.**

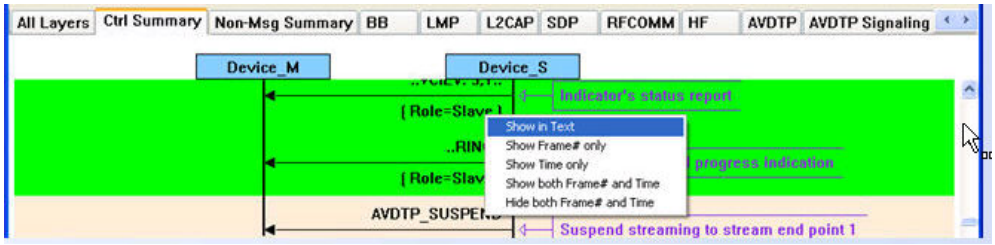


Figure 4.102 - Return to Text View Using Right-Click Menu

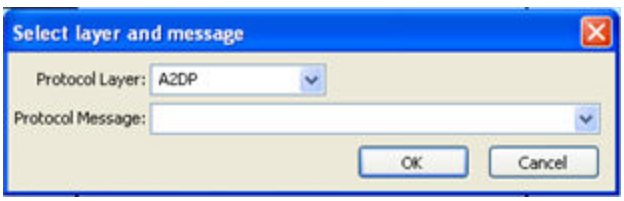
You can also choose to show:

- Frame # only
- Time only
- Show both Frame# and Time
- Hide both Frame# and Time

4.4.5.1 Message Sequence Chart - Search

The Message Sequence Chart has a Search function that makes it easy to find a specific type message within the layers.

When you select the 1) **Search** icon or 2) use **F3** key, the **Select layer and message** dialog appears.



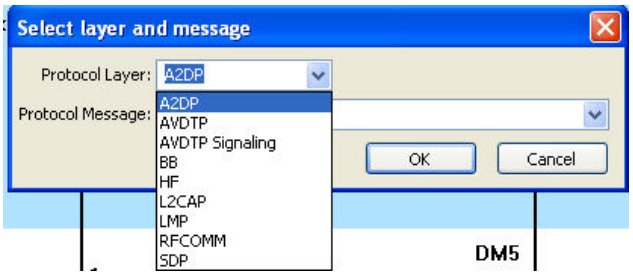
From this dialog you can search for specific protocol messages or search for the first error frame.

1. On the MSC dialog select one of the protocol tabs at the top.

Note: If you select **All Layers** in Step 1, the Protocol Layers drop-down list is active. If you select any of the other single protocols, the Protocol Layers drop-down is grayed out.

2. Or Open the Search dialog using the Search icon or the **F3** key.
3. Select a specific Protocol Message from the drop-down list.
4. Once you select the Protocol Message, click **OK**

The Search dialog disappears and the first search result is highlight in the Message Sequence Chart.



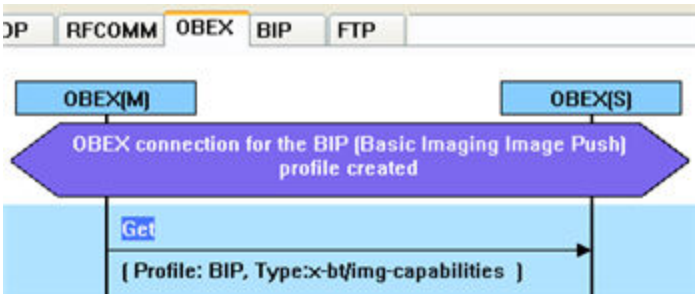


Figure 4.103 - Highlighted First Search Result

If there is no instance of the search value, you see this following dialog.

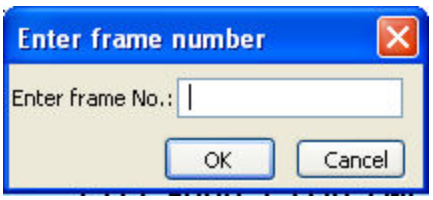
Once you have set the search value, you can 1) use the **Search Previous** and **Search Next** buttons or 2) **F2** and **F4** to move to the next or previous frame in the chart.

4.4.5.2 Message Sequence Chart - Go To Frame

The **Message Sequence Chart** has a **Go To Frame** function that makes it easy to find a specific frame within the layers.

In addition to Search, you can also locate specific frames by clicking on the **Go To Frame** toolbar icon.

1. Click **Go To Frame** in the toolbar.
2. Enter a frame number in the **Enter frame No.:** text box.
3. Click **OK**.

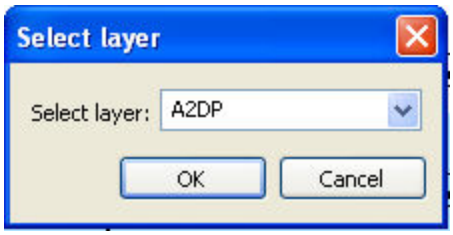


The Go To Frame dialog disappears and the selected frame is highlighted in the chart.

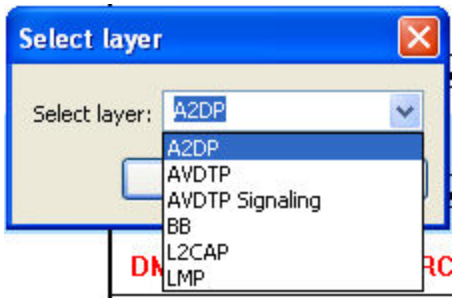
Once you have identified the frame in Go To, you can 1) use the Search Previous and Search Next buttons or 2) **F2** and **F4** keys to move to the next or previous frame in the chart.

4.4.5.3 Message Sequence Chart - First Error Frame

When you select **Go to first error frame** from the toolbar , the **Select layer** dialog appears.



You have to select a layer from the drop down list to choose what layer you want to search for the error.



Once you select a layer, then **OK**, the first error for that layer will be displayed.

If no error is found, a dialog will announce that event.

4.4.5.4 Message Sequence Chart - Printing

There are three standard MSC print buttons. **Print Preview**, **Print**, and **Cancel Printing**.

Print Preview

1. When you select **Print Preview** , the **Print Setup** dialog appears.
2. You next need to select your printer from the drop-down list, set printer properties, and format the print output..
3. Then you select **OK**.

After you select **OK**, the **Message Sequence Chart Print Preview** dialog appears.

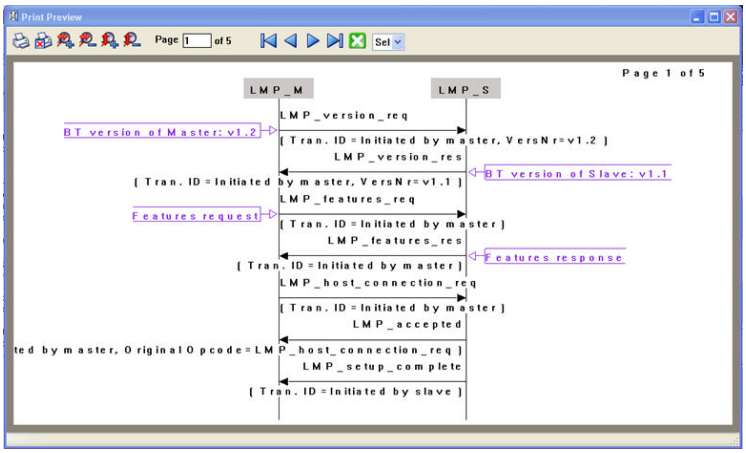


Figure 4.104 - Message Sequence Chart Print Preview

The information in the dialog will vary depending on the layer that is selected in the Message Sequence Chart, the properties of the printer you select, and the amount of data in the layer (which will correspond to the number of pages displayed).

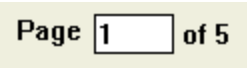
You control what you see and when to print using the toolbar at the top of the dialog.

Figure 4.105 - Print Preview Toolbar

Table 4.16 - Print Preview Icons

Icon	Name	Description
	Print	Prints all the pages to the printer you select in Print Setup dialog. When you select Print, you will output the data that is currently being displayed.
	Cancel Printing	Cancels the current printing.

Table 4.16 - Print Preview Icons (Continued)

Icon	Name	Description
	Zoom In Horizontially	Expands the data horizontally so it can be easier to read.
	Zoom Out Horizontally	Squeezes the data together so that more fits on one page.
	Zoom In Vertically	Expands the data vertically so it can be easier to read.
	Zoom Out Vertically	Squeezes the data so that more fits on one page.
	Current Page	The current page text box displays the page number this is currently shown in the dialog. You can enter a number in the text box, then press Enter, and the dialog will display the data for that page.
	Page navigation	If the data requires multiple pages, the navigation buttons will take you to: • The first page • The previous page • The next page • The last page
	Close Print Preview	Closes the dialog and returns to the Message Sequence Chart
	Select Font Size	Allows selection of the print font size from the drop-down control.

4.5 Packet Error Rate Statistics

The **Packet Error Rate** (PER) Stats view provides a dynamic graphical representation of the Packet Error Rate for each channel. The dialog displays a graph for each Classic Bluetooth® channel numbered 0 through 78 and for each *Bluetooth* low energy channel numbered 0 through 39.

Packet Error Rate Stats assist in detecting bad communication connections. When a high percentage of re-transmits, and/or header/payload errors occur, careful analysis of the statistics indicate whether the two devices under test are experiencing trouble communicating, or the packet sniffer is having difficulty listening.

Generally, if the statistics display either a large number of re-transmits with few errors or an equal number of errors and re-transmits, then the two devices are not communicating clearly. However, if the statistics display a large number of errors and a small number of re-transmits, then the packet sniffer is not receiving the transmissions clearly.

You can access this window in Classic Bluetooth® by selecting the **Classic *Bluetooth* Packet Error Rates Statistics** icon from the **Control** window or **Frame Display**. You can access this window in *Bluetooth* low energy by selecting the ***Bluetooth* low energy Packet Error Rates Statistics** icon from the **Control** window or **Frame Display**. You can also open the window from the View menu on the same windows.

Classic *Bluetooth* Packet Error Rate

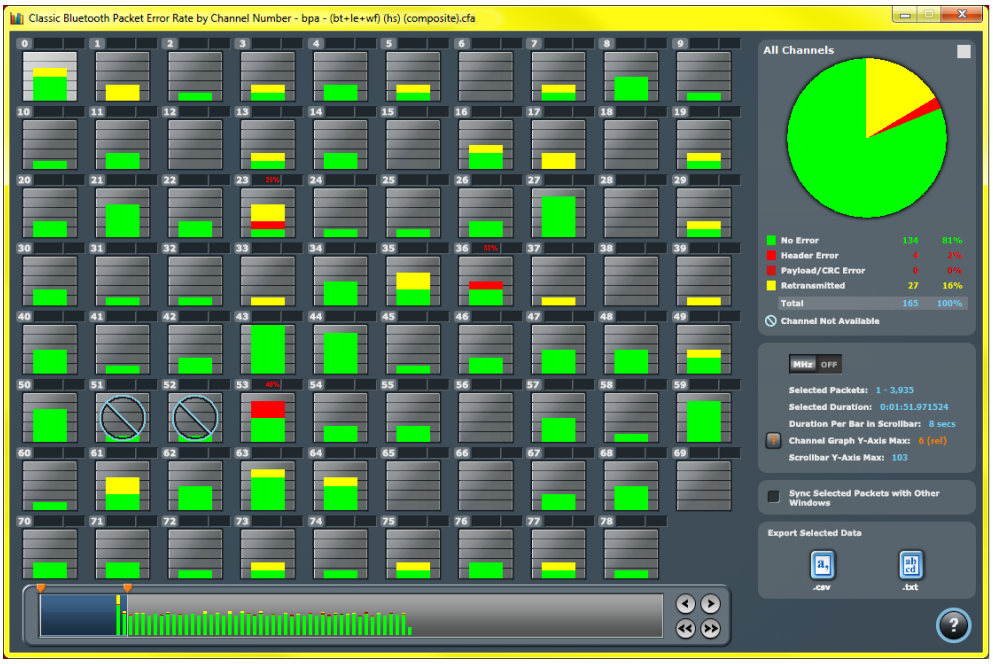


Figure 4.106 - Classic *Bluetooth* PER Stats Window

Bluetooth low energy Packet Error Rate

Figure 4.107 - *Bluetooth* low energy PER Stats Window

4.5.1 Packet Error Rate - Channels (Classic and low energy)

The main portion of the PER Stats dialog displays the 79 individual channels, 0-78, for Classic Bluetooth® and 40 individual channels, 0-39, for *Bluetooth* low energy.

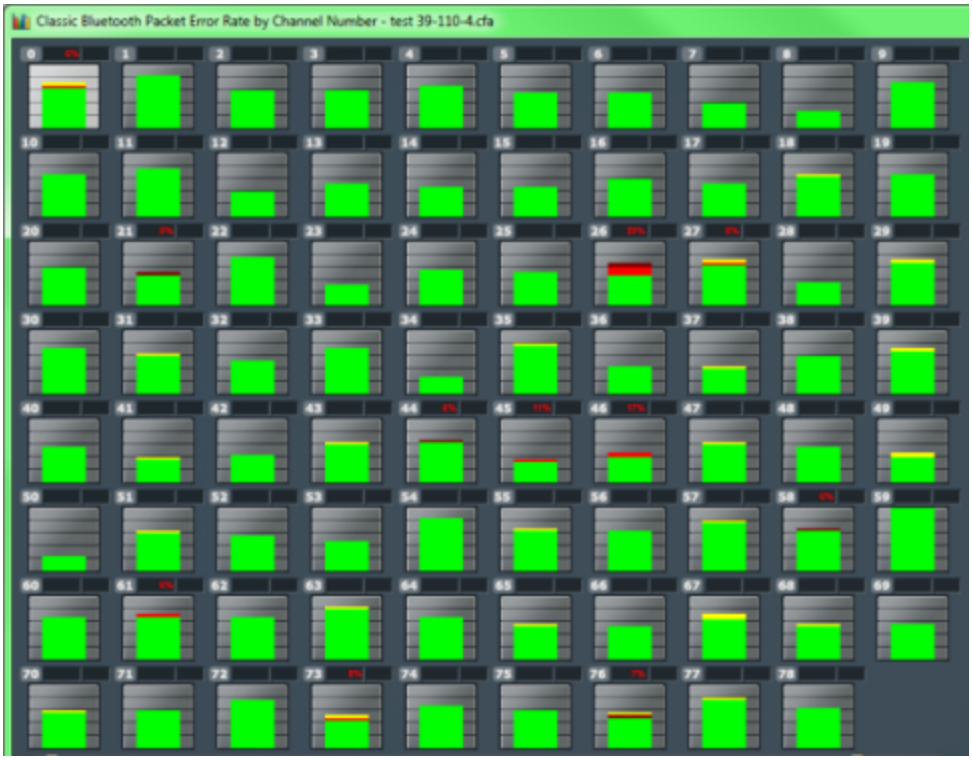


Figure 4.108 - Classic *Bluetooth* Packet Error Rate Channels

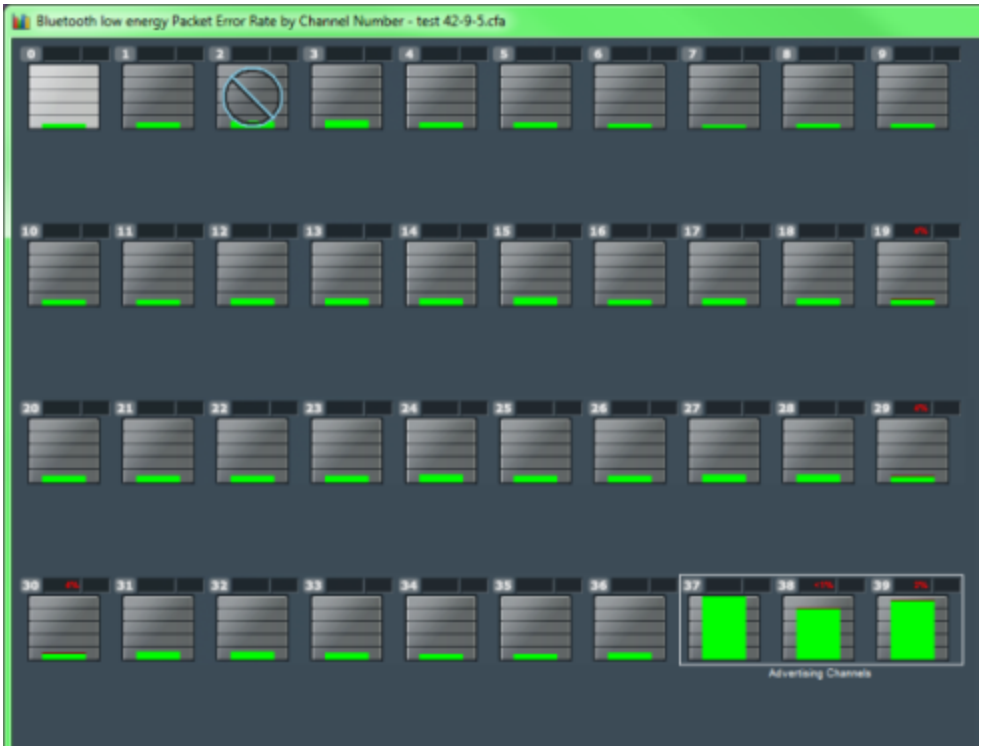


Figure 4.109 - *Bluetooth* low energy Packet Error Rate Channels

- **For Classic *Bluetooth:*** Each channel contains a bar that displays the number of packets with no errors in green, packets with Header Errors in red, packets with Payload or CRC errors in dark red, and Retransmitted packets in yellow.
- The red number at the top of the channel shows the percentage of Header Error and Payload/CRC Errors in relationship to the total number of packets in the channel.
- The light blue number at the top of each channel shows the megahertz (MHz) for the channel if the option is chosen in the Additional Statistics section.
- When you select a channel, detailed information for that channel is displayed in the expanded chart on the upper right.
- The channels change dynamically as the Viewport is moved or new data appears within the Viewport.
- The **Channel Not Available** symbol is displayed if the channel is not available in the most recent channel map that is in or before the last selected packet, even if that channel map comes before the first selected packet. *Bluetooth* Adaptive Frequency Hopping processes will block channels determined to be unreliable. These channels are not available because the Bluetooth devices have decided not to use them.

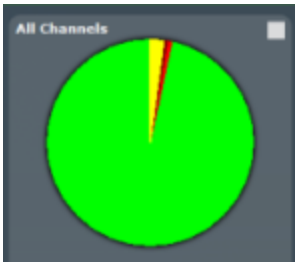
- "s" changes the size of the entire dialog.
- "c" changes the contrast of the dialog
- The **Reset** button is only available in live mode. The button will appear in the lower right-hand corner of the Channels section. Clicking on the **Reset** button will clear all prior data from PER Stats.

4.5.2 Packet Error Rate - Pie Chart and Expanded Chart

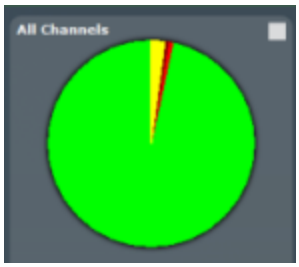
The **Expanded PER Stats Chart** (in the upper right) displays detailed information about the channel selected from the main channel dialog.

Expanded Chart

Pie Chart



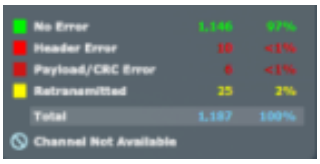
- When PER Stats is first opened, Channel 0 is displayed in the expanded chart.
- The top orange number on the Y-Axis displays the maximum number of packets in Snap Mode. If Snap Mode is turned off, the number will display in light blue.
- The number of the selected channel is displayed in the upper-left corner of the expanded chart.
- The combined value of Header and Payload/CRC errors for the channel is displayed in red as a percentage to the right of the channel number.
- The megahertz (MHz) value is displayed in light blue text if the MHz option is selected in the Additional Statistics section.
- The number of packets with no errors is displayed in light green in the bar chart.
- **For Classic Bluetooth®** : The number of packets that have header errors is displayed in red in the bar chart.
- **For Classic *Bluetooth***: The number of payload errors is displayed in dark red in the bar chart.
- **For Classic *Bluetooth***: The number of re-transmits is displayed in yellow in the bar chart.
- All the values, except MHz, change dynamically when multiple time periods are selected in the Scroll Bar.
- When you select the in the upper-right corner, the bar chart is replaced by a pie chart. The pie chart applies to all channels, not a selected channel. To return to the bar chart, click on the channel again or click on the in the upper right hand corner.



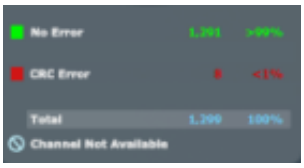
4.5.3 Packet Error Rate - Legend

The **Legend** displays color coded information about the channel selected.

Classic Bluetooth®



Bluetooth low energy



For Classic *Bluetooth*

- The number of Packets with **No Errors** and percentage of packets with **No Errors** in relationship to total packets for the channel is displayed in green.
- The number of Packets with **Header Errors** and percentage of packets with **Header Errors** in relationship to total packets for the channel is displayed in red.

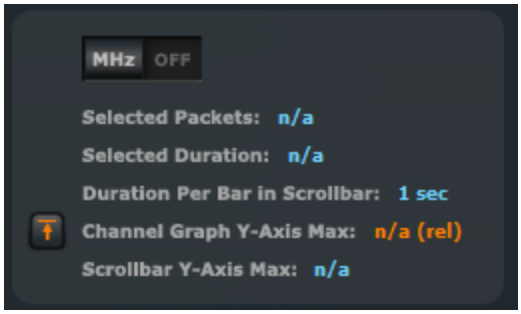
- The number of Packets with **Payload/CRC Errors** and percentage of packets with **Payload/CRC Errors** in relationship to total packets for the channel is displayed in dark red.
- The number of **Retransmitted** Packets and percentage of **Retransmitted** packets in relationship to total packets for the channel is displayed in yellow.
- **Total** packets and **Total** percentage is displayed in light blue.

For *Bluetooth* low energy:

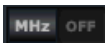
- The number of Packets with **No Errors** and percentage of packets with **No Errors** in relationship to total packets for the channel is displayed in green.
- The number of Packets with **CRC Errors** and percentage of packets with **CRC Errors** in relationship to total packets for the channel is displayed in dark red.
- **Total** packets and **Total** percentage is displayed in light blue.

For a description of the **Channel Not Available** symbol, see PER Stats Channel.

4.5.4 Packet Error Rate - Additional Statistics


MHz OFF
Selected Packets: n/a
Selected Duration: n/a
Duration Per Bar in Scrollbar: 1 sec
Channel Graph Y-Axis Max: n/a (rel)
Scrollbar Y-Axis Max: n/a

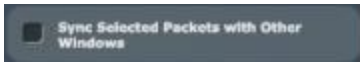
This Additional Statistics section of PER Stats displays information about selected packets, duration, and Y-Axis max, and it also has two controls.

- Selecting **MHz On** displays the megahertz value for each channel in the main channels chart and also in the expanded chart.
- Selecting **MHz Off**  removes the megahertz value.
- **Selected Packets** displays the packet range selected in the Scroll Bar. This includes inapplicable Inapplicable packets include Wi-Fi packets, Sniffer Debug packets, any packets that are not relevant to PER Stats. Inapplicable packets do not appear as part of the Additional Statistics. packets.
- **Selected Duration** identifies the total amount of time in the selected packet range displayed in the Scroll Bar.
- **Duration Per Bar in Scrollbar:** identifies the amount of time represented by each bar in the Scroll Bar.
- The **Channel Graph Y-Axis Max** can display two different values. When the **Snap Arrow** is orange , the values for channels in the main chart are shown in relative terms in **Snap Mode**. This means that one channel (or channels) with the greatest value is "snapped" to the top of the chart. In the graphic below left, Channel 33 is snapped to the top of the chart.

The channel(s) with the greatest value become a full-scale reference display for the other channels that have been relatively scaled. Channel comparisons become easier. With Snap On you can select multiple time values in the Scroll Bar. When the **Snap Arrow** is white (Snap Mode turned off), the values for channels in the main chart are shown in absolute values where the max value of each channel graph is the same regardless of the position of the Viewport. Channel 33, which is snapped to the top of the chart in Snap Mode (shown above left), appears like the right image when Snap Mode is turned off.

- **Scrollbar Y-Axis Max** displays the maximum Y-Axis value in the Scroll Bar.

4.5.5 Packet Error Rate - Sync Selected Packets With Other Windows

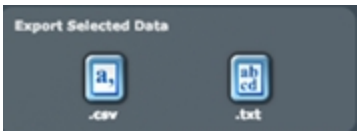


By default, and unlike other windows, PER Stats is not synchronized with other windows such as Frame Display in that selecting a frame range in one does not highlight the same frame range in the other. This ensures that Frame Display isn't constantly re-synchronizing during live capture while the view-port is maximized in PER Stats. If PER Stats synchronization is desired, it can be enabled by checking the **Sync Selected Packets with Other Windows** check box.

4.5.6 Packet Error Rate - Export

The Export section of PER Stats allows you to export data to a .csv or .txt file.

1. To use the Export, select a range of data using the Viewport.
2. Select .csv or .txt from **Export Selected Data**, depending on what type of data file you want. The **Save As** dialog appears.



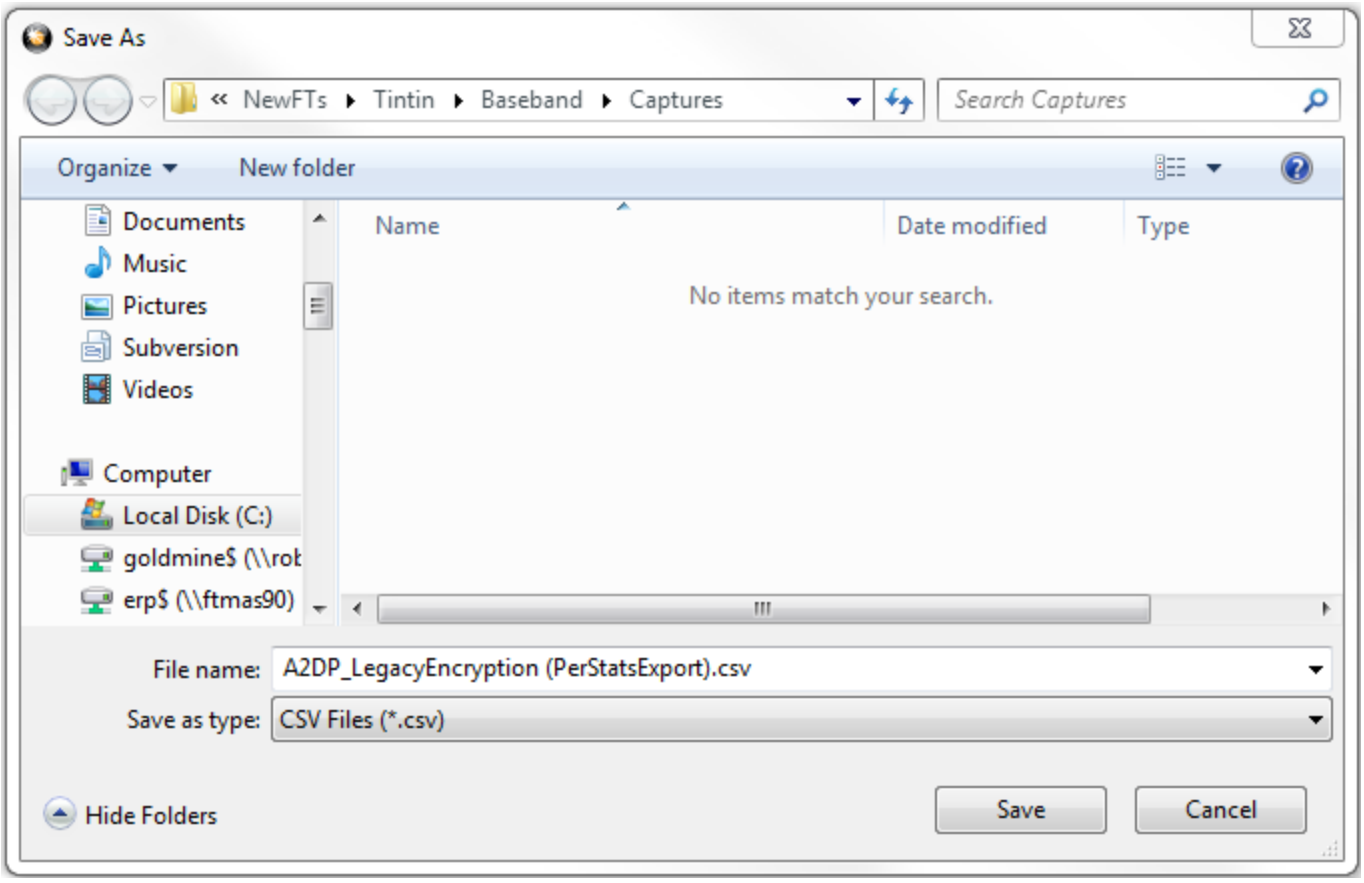


Figure 4.110 - Save As dialog in PER Stats Export

3. Select a location where you want to save the file in "Save in:".
4. Enter a file name in "File name:".
5. Select "Save".

The file will be saved to that location.

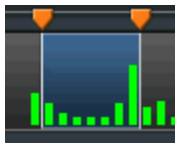
4.5.7 Packet Error Rate - Scroll Bar

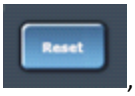
The PER Stats **Scroll Bar** displays stats for all packets, divided into equal time intervals.

Figure 4.111 - PER Stats Scroll Bar

- Captured data begins to appear on the left and fills the width of the bar, left to right.
- The vertical bars in the **Scroll Bar** each indicate a fixed duration. When data first appears in the **Scroll Bar** as it is being captured, each bar equals one second. When the data fills the bar, reaching the right side limit,

the last bar moves back to the center of the **Scroll Bar**. The bars stay the same size, but doubles in duration (for example, the first time the **Scroll Bar** fills, the bars return to the middle, but now each bar represent two seconds of time instead of one). Each time the bars cycle to the middle, the time they represent doubles. When the bars move and the **Viewport** (see below) is not maximized, the **Viewport** moves with the bars so that the same packet range is indicated. When the **Viewport** is maximized it stays maximized regardless of what the bars do. This ensures that the display can be made to reflect all packets at all times by maximizing the .

- The **Viewport** is used to select single or multiple vertical bars  .
- You can drag the sides of the **Viewport** or the slider buttons to select multiple bars, representing a greater time range.
- You can click and drag the **Viewport** within the **Scroll Bar**.
- When you select a packet range in **Frame Display** that includes only some of the frames in PER Stats, the **Viewport** snaps up against the side of the bar with the unselected frames .
- When you select a packet range in Frame Display that includes all of the frames in PER Stats, the Viewport displays a space between the Viewport sides and the bar .
- Double clicking anywhere inside the **Scroll Bar** selects the entire **Scroll Bar**. Double clicking again toggles back to the previous size of the **Viewport**.
- Selecting Ctrl+A is the same as double-clicking.
- Clicking on a vertical bar left justifies the **Viewport** to that bar.
- Shift-clicking on a bar extends the nearest **Viewport** side to include that bar.
- The Home key moves the **Viewport** to the left edge.
- The End key moves the **Viewport** to the right edge.
- Pressing the left arrow button , the left arrow key, or the up arrow key moves the **Viewport** to the left, one vertical bar at a time.
- Pressing the right arrow button . the right arrow key, or the down arrow key moves the **Viewport** to the right, one vertical bar at a time.
- Pressing the double left arrow button or the PgUp key moves the **Viewport** to the left by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.
- Pressing the double right arrow button or the PgDn key moves the **Viewport** to the right by the current width of the **Viewport**. Holding down the Shift key will prevent the **Viewport** from moving if there is not enough room to move by its full width.

- Holding the Shift key down and the right or left arrows moves the right side of the **Viewport**.
- Holding the Ctrl key down and the right or left arrows moves the left side of the **Viewport**.
- The Scroll bar includes inapplicable packets (sniffer debug, WiFi, etc) so that the packet range selected in Frame Display can be shown. Inapplicable packets are not, however, included in the statistics reports.
- If the **Viewport** is adjusted within PER Stats, as opposed to selecting a packet range in Frame Display, it uses only whole bars on both sides.
- Statistics are retained for all packets regardless of whether any of those packets have wrapped out. You can select the **Reset** button 

, which is located above the right portion of the **Scroll Bar**, to discard all stats for packets received up to that point.
- The **Reset** button is only available when you are capturing data.

4.5.8 Packet Error Rate - Excluded Packets

ID packets and packets that are missing channel numbers (such as HCI and BTSnoop) will not display data. ID packets are excluded because they can not have errors or indicate retransmission and therefore dilute the percentages for other packet types. Packets without channel numbers are excluded because the graphs are channel-specific. Before packets are captured, the Scroll Bar in Classic *Bluetooth* PER Stats contains the message "ID packets and packets without a channel number (such as HCI) are excluded", and the Scroll Bar in *Bluetooth* low energy PER Stats contains the message "Packets without a channel number (such as HCI) are excluded".

Figure 4.112 - Example: Excluded Packets Message in Scroll Bar (Classic *Bluetooth*)

4.6 Data/Audio Extraction

You use Data/Audio Extraction to pull out data from various decoded Bluetooth® protocols. Once you have extracted the data, you can save them into different file types, such as text files, graphic files, email files, .mp3 files, and more. Then you can examine the specific files information individually.

1. You access this dialog by selecting Extract Data/Audio from the View menu or by clicking on the icon from the toolbar .

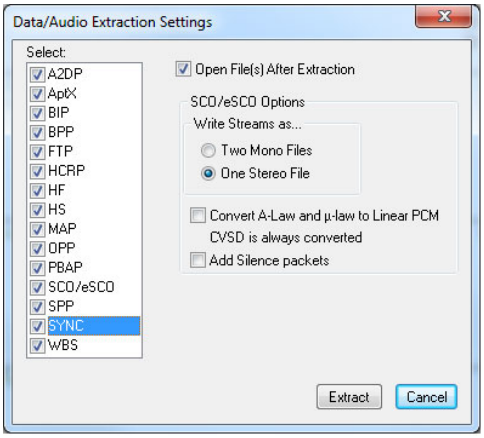


Figure 4.17 Data/Audio Extraction Settings dialog

2. Choose a checkbox(es) on the left side of the dialog to identify from which profile(s) you want to extract data.

   It's important to note that if there is no data for the profile(s) you select, no extracted file is created.

3. If you want the file(s) to open automatically after they are extracted, select the **Open File(s) After Extraction** checkbox.

   Note: This does not work for SCO/eSCO.

4. Click on a radio button to write the streams as **Two Mono Files** or as **One Stereo File**.

   Note: This option is for SCO/eSCO only.

5. Select the checkbox if you want to convert **A-Law and µ-law to Linear PCM.** CVSD are always converted to Linear PCM. It's probably a good idea to convert to Linear PCM since more media players accept this format.

   Note: This option is for SCO/eSCO only.

6. Select the **Add Silence packets** to insert the silence packets (dummy packets) for the reserved empty

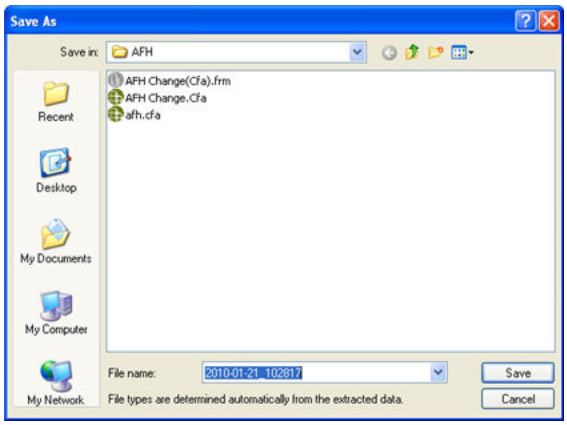
slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots.

Note: This option is for SCO/eSCO only.

7. Select **Extract.**

   A **Save As** dialog appears.

   The application will assign a file name and file type for each profile you select in Step 1 above. The file type varies depending on the original profile. A separate file for each profile will be created, but only for those profiles with available data.



8. Select a location for the file.

9. Click **Save**.

   The **Data Extraction Status** and **Audio Extraction Status** dialogs appear. When the process is complete the dialogs display what files have been created and where they are located.

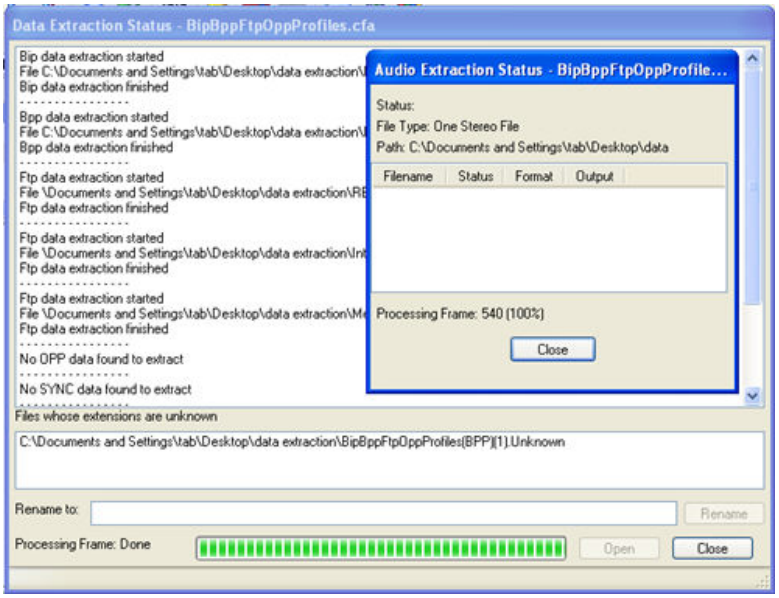


Figure 4.18 Data and Audio Extraction Status

   If you selected **Open Files(s) After Extraction**, the files open automatically.

10. If you did not select this option, you can open a file by simply double-clicking on the name.

Also, if a file type is unknown, you can select the file and it appears in the **Rename to**: text box.

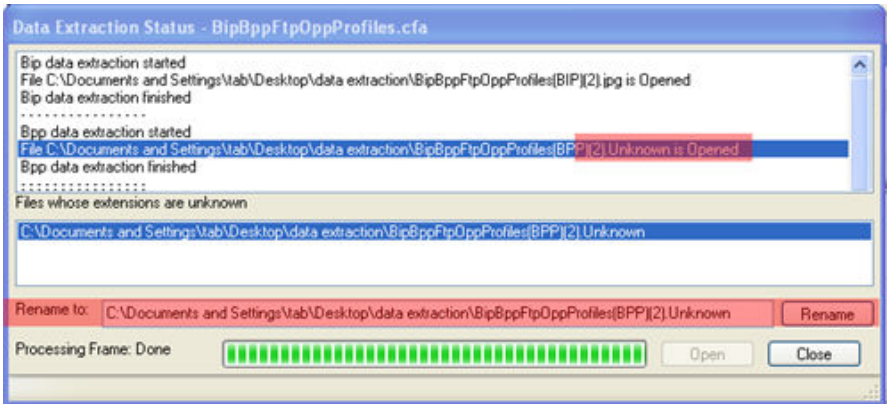


Figure 4.19 Rename To in the bottom section of Data Extraction Status

Then you can rename the file, adding a file type to attempt to open the file.

When you are finished, select **Close** to close the dialogs.

Chapter 5 Navigating and Searching the Data

The following sections describe how to navigate through the data and how to find specific data or packet conditions of interest to the user.

5.1 Find

Capturing and decoding data within the ComProbe analyzer produces a wealth of information for analysis. This mass of information by itself, however, is just that, a mass of information. There has to be ways to manage the information. ComProbe software provides a number of different methods for making the data more accessible. One of these methods is **Find**.

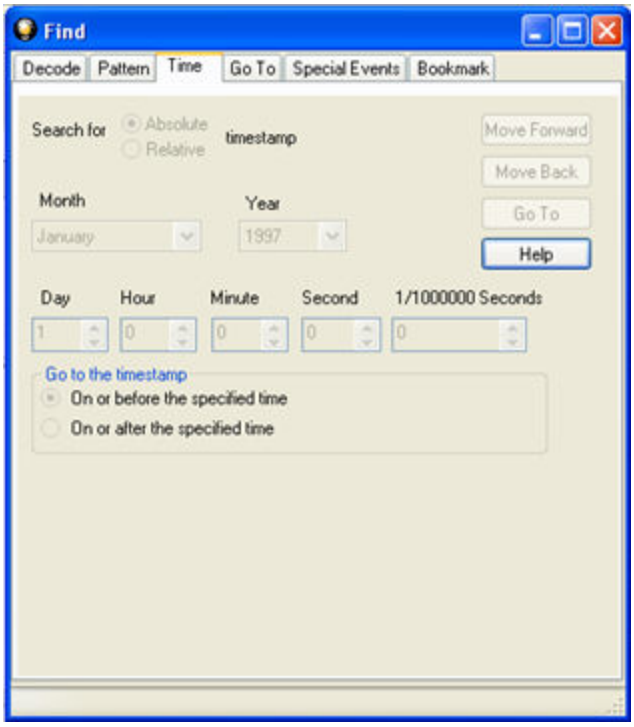


Figure 5.1 - Find Dialog

Find, as the name suggests, is a comprehensive search function that allows users to search for strings or patterns in the data or in the frame decode. You can search for errors, control signal changes, bookmarks, special events, time, and more. Once the information is located, you can easily move to every instance of the Find results.

5.1.1 Searching within Decodes

Searching within decodes lets you to do a string search on the data in the **Decode Pane** of the **Frame Display** window.

To access the search within decodes function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Decode** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

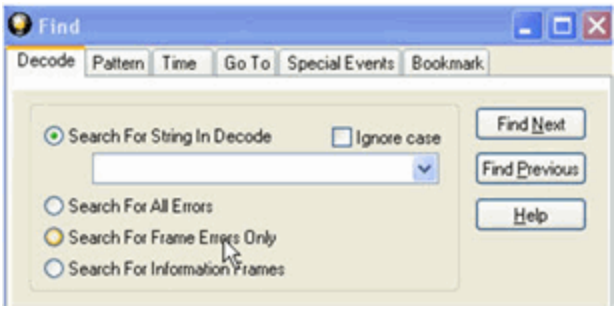


Figure 5.2 - Find Decode Tab Search for String

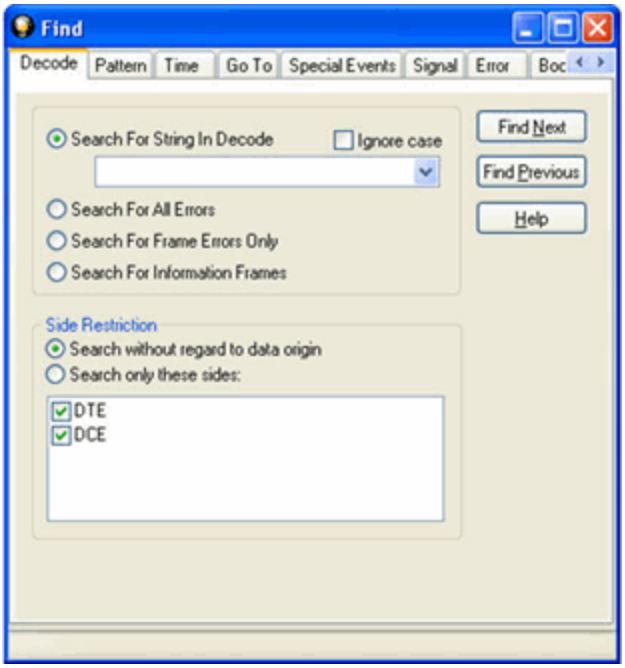


Figure 5.3 - Find Decode Tab Side Restriction

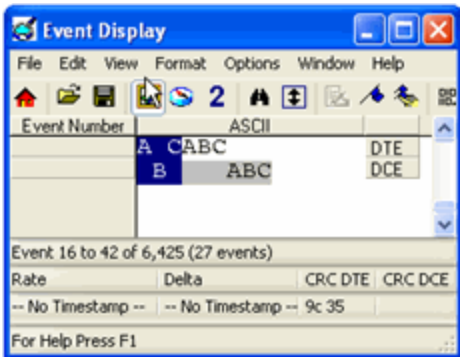
There are several options for error searching on the **Decoder** tab.

- **Search For String in Decoder** allows you to enter a string in the text box. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the analyzer saves the search. The next time you open **Find**, the drop-down list will contain your search parameters.
- **Search for All Errors** finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- **Search for Frame Errors Only** finds frame specific errors, such as frame check errors.
- **Search for Information Frame** only searches information frames.

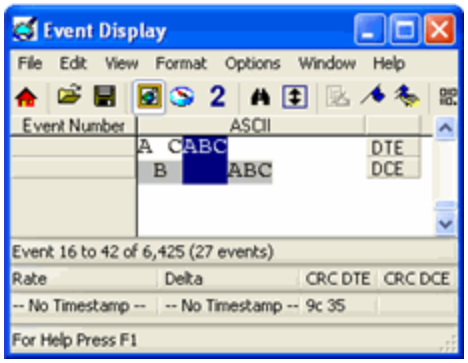
1. Enter the search string.
2. Check **Ignore Case** to do a case-insensitive search.
3. When you have specified the time interval you want to use, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the **Decode** pane in **Frame Display.**

Side Restrictions - **Side Restriction** means that the analyzer looks for a pattern coming wholly from the DTE or DCE side. If you choose to search without regard for data origin, the analyzer looks for a pattern coming from one or both sides. For example, if you choose to search for the pattern ABC and you choose to search without regard for data origin, the analyzer finds all three instances of ABC shown here.



The first pattern, with the A and the C coming from the DTE device and the B coming from the DCE is a good example of how using a side restriction differs from searching without regard to data origin. While searching without regard for data origin finds all three patterns, searching using a side restriction never finds the first pattern, because it does not come wholly from one side or the other.



If you choose to search for the pattern ABC, and you restrict the search to just the DTE side, the analyzer finds the following pattern:

In this example, the analyzer finds only the second pattern (highlighted above) because we restricted the search to just the DTE side. The first pattern doesn't qualify because it is split between the DTE and DCE sides, and the third pattern, though whole, comes from just the DCE side.

If we choose both the DTE and the DCE sides in the above example, then the analyzer finds the second pattern followed by the third pattern, but not the first pattern. This is because each side has one instance in which the whole pattern can be found. The analyzer completely searches the DTE side first, followed by the DCE side.

Note: Side Restriction is available for pattern and error searching.

1. Select one of the two options.
2. Select **DTE**, **DCE**, or both.
3. When you made your selections, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the **Decode** pane in **Frame Display.**

5.1.2 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards.

To access the search by pattern function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.

3. Click on the **Find** icon or choose **Find** from the **Edit** menu.

4. Click on the **Pattern** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

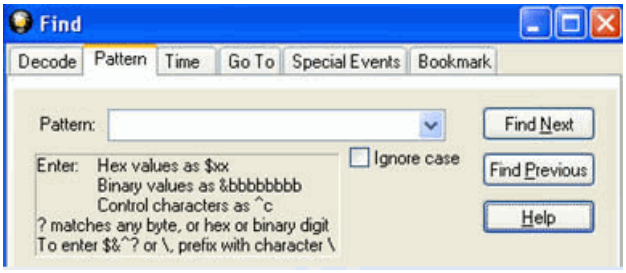


Figure 5.4 - Find Pattern Tab

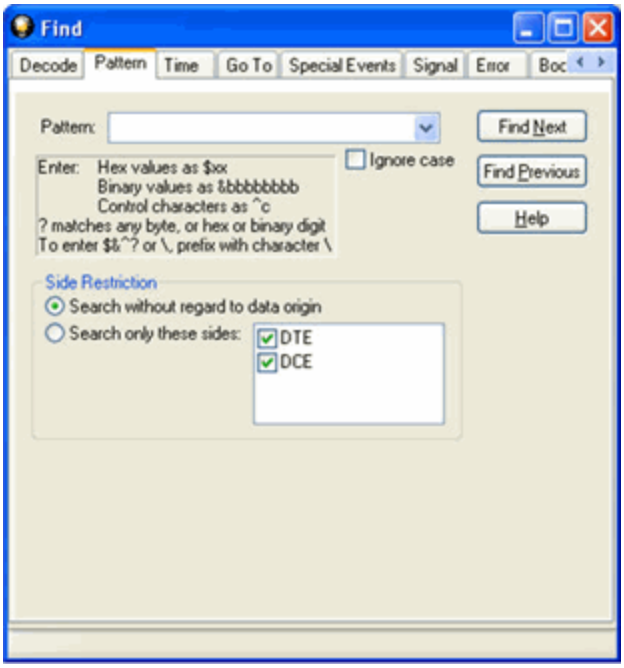


Figure 5.5 - Find Pattern Tab Side Restrictions

Pattern allows you to enter a string in the text box. You can use characters, hex or binary digits, control characters, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the ComProbe analyzer saves the search. The next time you open **Find**, the drop-down list will contain your search parameters.

1. Enter the search pattern.

2. Check **Ignore Case** to do a case-insensitive search.

3. When you have specified the pattern you want to use, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the in Frame Display and Event Display.

Refer to Searching by Decode on page 194 for information on **Side Restrictions**

5.1.3 Searching by Time

Searching with **Time** allows you search on timestamps on the data in **Frame Display** and **Event Display** window.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Time** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

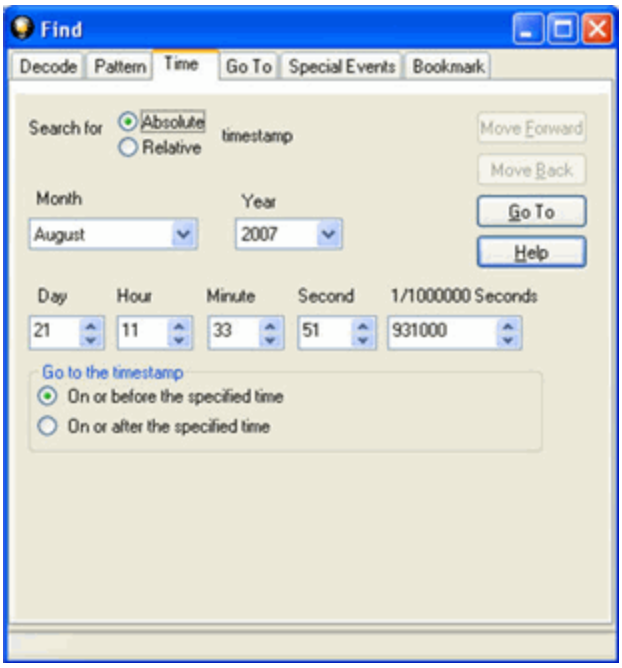


Figure 5.6 - Find by Time tab

The analyzer can search by time in several different ways.

Search for Absolute/Relative timestamp.

- Absolute - An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.
- Relative - A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

1. Select **Absolute** or **Relative**
2. Select the date and time using the drop-down lists for **Month**, **Year**, **Day**, **Hour**, **Minute**, **Second**, 1/**10000000**.

Note: Month and Year are not available if you select Relative.

3. When you have specified the time interval you want to use, click on the **Go To**, **Move Forward** or **Move Backward** buttons to start the search from the current event.

Note: When you select **Absolute** as **Search for**, **Go To** is available. When you select **Relative** as **Search for**, **Move Forward** or **Move Backward**is available.

Go to the timestamp: On or before/ On or after

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the **Go to the timestamp** box.

If you are searching forward in the buffer, you usually want to choose the **On or After** option. If you choose the **On or Before** option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

When you select **Absolute** as **Search for**, the radio buttons are **On or before the specified time** or **On or after the specified time**. When you select **Relative** as **Search for**, the radio buttons are **On or before the specified time relative to the first selected item** or **On or after the specified time relative to the last selected item.**

1. Select **On or before the specified time** or **On or after the specified time**.
2. When you have specified the time interval you want to use, click on the **Go To**, **Move Forward** or **Move Backward** buttons to start the search from the current event.

   When you select **Absolute** as **Search for**, **Go To** is available. When you select **Relative** as **Search for**, **Move Forward** or **Move Backward**is available.

There are a couple of other concepts to understand in respect to searching with timestamps.

- The analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

- Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.
- The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.1.4 Using Go To

Searching with Go To allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Go To** tab of the **Find** dialog.
5. The system displays the **Find** dialog with the **Go To** tab selected.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

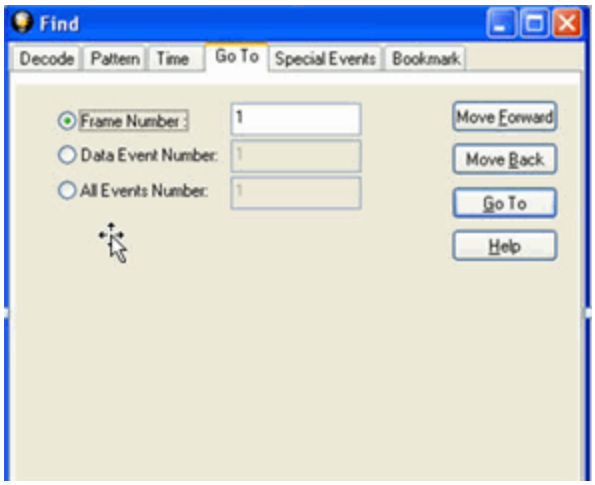


Figure 5.7 - Find Go To tab

To go to a particular frame :

1. Select the **Frame Number** radio button
2. Type the frame number in the box.
3. Click the **Go To** button.

4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the **Move Forward** or **Move Back** button.

To go to a particular event :

1. Select the **Data Event Number** or **All Events Number** radio button.
2. Type the number of the event in the box.
3. Click the **Go To** button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the **Move Forward** or **Move Backward** button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on **Move Forward**. Each time you click on **Move Forward,** Frontline moves forward 10 events.

See Event Numbering for why the **Data Event Number** and **All Events Number** may be different. As a general rule, if you have the **Show All Events** icon depressed on the **Event Display** window or **Frame Display Event** pane, choose **All Events Number**. If the **Show All Events** button is up, choose **Data Event Number**.

5.1.5 Searching for Special Events

Frontline inserts or marks events other than data bytes in the data stream. For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker. You can use Find to locate single or multiple special events.

To access the search for special events function:

1. Open a capture file to search.
2. Open the Event Display or Frame Display window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Special Events** tab of the Find dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

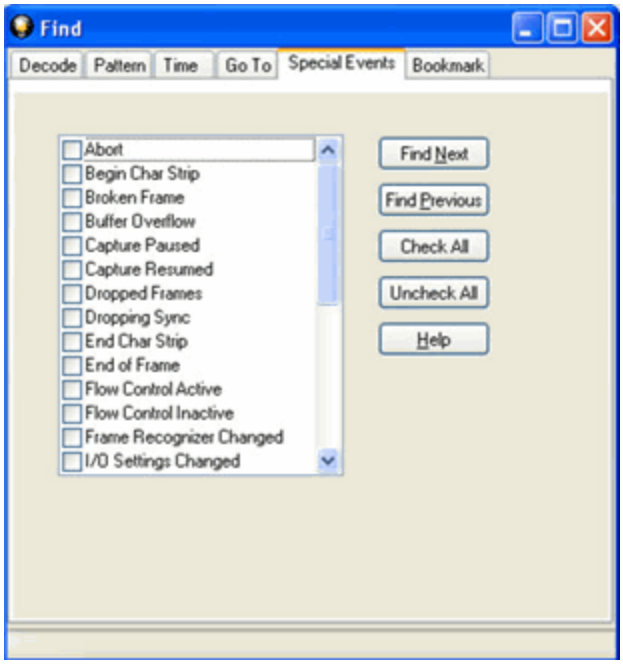


Figure 5.8 - Find Special Events tab

5. Check the event or events you want to look for in the list of special events. Use **Check All** or **Uncheck All** buttons to make your selections more efficient.
6. Click Find Next and Find Previous to move to the next instance of the event.

Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of all Event Symbols on page 72.

5.1.6 Searching by Signal

Searching with Signal allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where control signals changed.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Signal** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

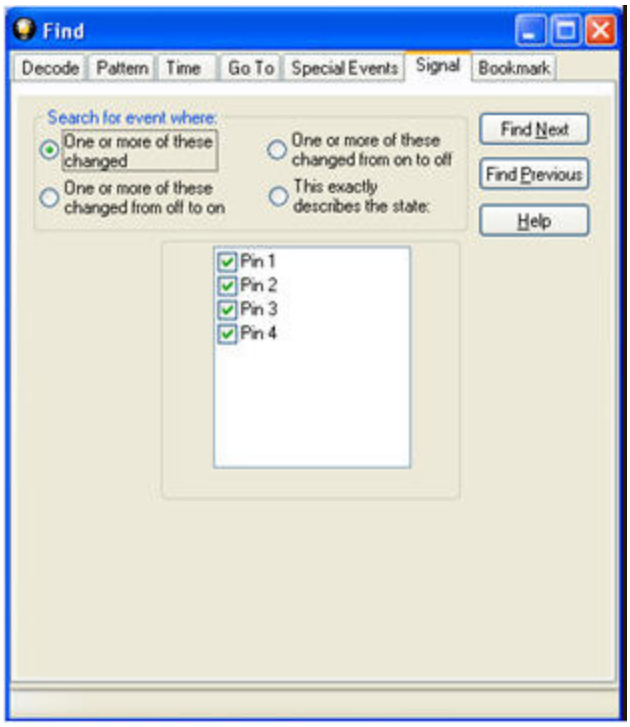


Figure 5.9 - Find Signal tab.

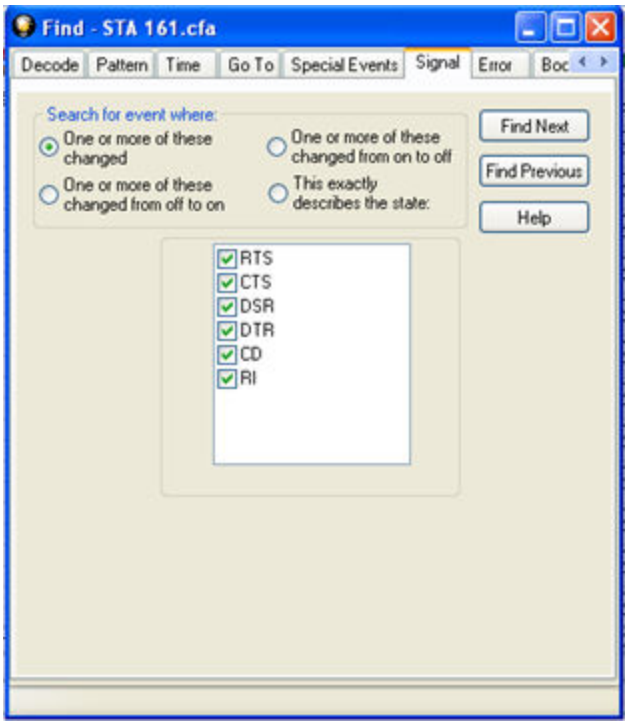


Figure 5.10 - Find Signal Tab

You will choose one qualifier—**Searching for event where**, then choose one or more control signals

Control Signals

The section with the check boxes allows you to specify which control signals the analyzer should pay attention to when doing the search. The analyzer pays attention to any control signal with a check mark.

- Click on a box to place a check mark next to a control signal
- Click again to uncheck the box
- By default, the analyzer searches all control signals, which means all boxes start out checked.

For example, if you are only interested in finding changes in **RTS** and **CTS**, you would check those two boxes and uncheck all the other boxes. This tells the analyzer to look only at the **RTS** and **CTS** lines when running the search. The other signals are ignored.

The control signals types include:

- USB - Pin 1
- USB - Pin 2
- USB - Pin 3
- USB - Pin 4

or

- RS232 - Request to Send (RTS)
- RS232 - Clear to Send (CTS)
- RS232 - Data Set Ready (DSR)
- RS232 - Data Terminal Ready (DTR)
- RS232 - Carrier Detect (CD)
- RS232 - Ring Indicator (RI).

Click here to learn more about the Breakout Box and Pins 1 - 4.

Searching for event where:

- The first three options are all fairly similar, and are described together. These options are searching for an event where:
    - One or more control signals changed
    - One or more control signals changed from off to on
    - One or more control signals changed from on to off
- Searching for an event where one or more signals changed means that the analyzer looks at every control signal that you checked, and see if any one of those signals changed state at any time.

- If you want to look at just one control signal:
  - Check the box for the signal.
  - Uncheck all the other boxes.
  - Choose to search for an event where one or more signals changed.
  - The analyzer notes the state of the selected signal at the point in the buffer where the cursor is, search the buffer, and stop when it finds an event where RTS changed state.
  - If the end of the buffer is reached before an event is found, the analyzer tells you that no matches were found.

- Searching for events where control signals changed state from off to on, or vice versa, is most useful if the signals are usually in one state, and you want to search for occasions where they changed state.

  For example:

  - If DTR is supposed to be on all the time but you suspect that DTR is being dropped
  - Tell the analyzer to look only at DTR by checking the DTR box and unchecking the others
  - Do a search for where one or more control signals changed from on to off.
  - The analyzer would search the DTR signal and stop at the first event where DTR dropped from on to off.

- Searching for an Exact State

  To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.

  - First, choose to search for an event where your choices exactly describe the state.
  - This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each control signal.
  - Choose which state you want each control signal to be in.
  - Choose Don't Care to have the analyzer ignore the state of a control signal.
  - When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.
  - If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
  - If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.
  - Select one of the four radio buttons to choose the condition that must be met in the search
  - Select one or more of the checkboxes for Pin 1, 2, 3, or 4.
  - Click **Find Next** to locate the next occurrence of the search criteria or **Find Previous** to locate an earlier occurrence of the search criteria.

5.1.7 Searching for Data Errors

The analyzer can search for several types of data errors. Searching for data error sallows you to choose which errors you want to search for and whether to search the DTE or DCE data or both. Bytes with errors are shown in red in the **Event Display** window, making it easy to find errors visually when looking through the data.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Errors** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

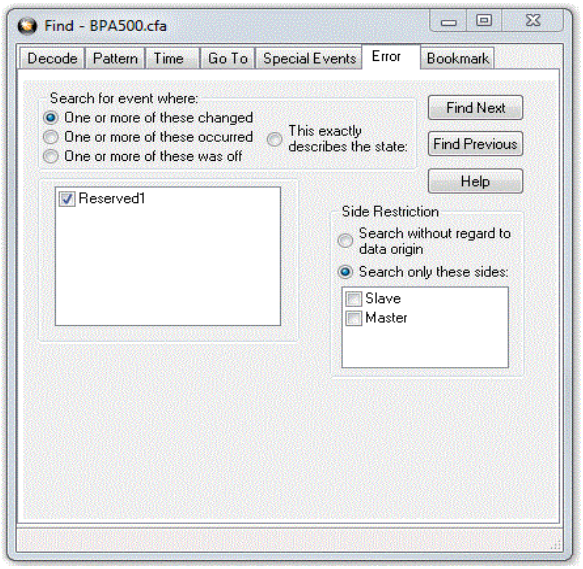


Figure 5.11 - Find Error tab.

Searching for event where

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- one or more error conditions changed
- one or more error conditions occurred
- one or more error conditions were off (i.e. no errors occurred)

Selecting Which Errors to Search

The section with the check boxes allows you to choose which errors the analyzer should look for. Click on a box to check or un-check it.

If you want to search only for overrun errors

- check the box if shown
- un-check the other boxes.

To search for all types of errors

- check all boxes

The most common search is looking for a few scattered errors in otherwise clean data.

To do this type of search:

- choose to **Search for an event where** one or more error conditions occurred
- choose which errors to look for
- By default, the analyzer looks for all types of errors.

In contrast, searching for an event where one or more error conditions were off means that the analyzer looks for an event where the errors were not present.

For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches the file, and finds the point at which framing errors stopped occurring.

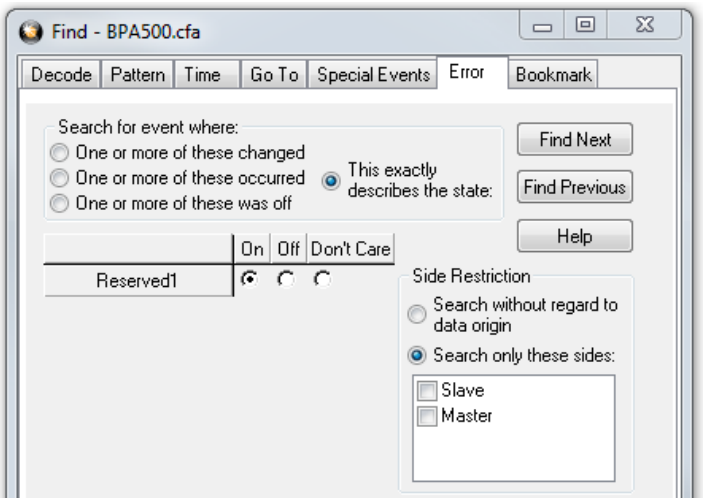
Searching for an event where the error conditions changed means that the analyzer searches the data and stop at every point where the error condition changed from on to off, or off to on.

For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click **Find Next,** the analyzer stops at the point when the errors began occurring again. Clicking **Find Previous** will search backwards from the current postion.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where error conditions changed. The analyzer searches until it finds an event where error conditions changed or it reaches the end of the buffer, at which point the analyzer tells you that there are no more events found in the buffer. If you are searching for an exact match, the analyzer asks you if you want to continue searching from the beginning of the buffer.

Searching for Exact Error Conditions

To search for an exact state means that the analyzer finds events that exactly match the error conditions that you specify.



- Select the **This exactly describes the state** radio button.
- This changes the normal check boxes to a series of radio buttons labeled **On**, **Off** and **Don't Care** for each error.
  - **On** means that the error occurred
  - **Off** means that the error did not occur
  - **Don't Care** means that the analyzer ignores that error condition.
- Select the appropriate state for each type of error.

Example:

If you need to find an event where just an overrun error occurred, but not any other type of error, you would choose overrun error to be On, and set all other errors to Off. This causes the analyzer to look for an event where only an overrun error occurred.

If you want to look for events where overrun errors occurred, and other errors may have also occurred but it really doesn't matter if they did or not, choose overrun to be On, and set the others to Don't Care. The analyzer ignores any other type of error, and find events where overrun errors occurred.

To find the next error, click the Find Next button. To find an error that occurred earlier in the buffer to where you are, click the Find Previous button.

5.1.8 Find - Bookmarks

Searching with **Bookmarks** allows you search on specific bookmarks on the data in **Frame Display** and **Event Display** window. Bookmarks are notes/reminders of interest that you attach to the data so they can be accessed later.

To access the search for bookmarks

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Bookmarks** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

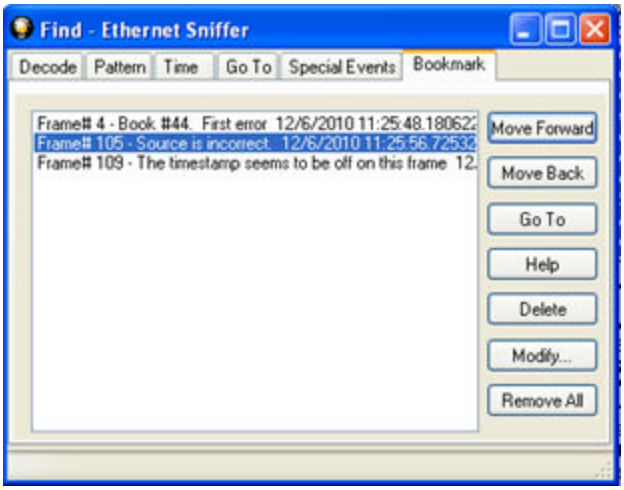


Figure 5.12 - Find Bookmark tab.

There are several ways to locate bookmarks.

- Select the bookmark you want to move to and click the **Go To** button.
- Simply double-click on the bookmark.
- Click the **Move Forward** and **Move Back** buttons to move through the frames to the bookmarks shown in the window. When the bookmark is found it is highlighted in the window.

There are three ways to modify bookmarks:

1. Click on **Delete** to remove the selected bookmark.
2. Click on **Modify...** to change the selected Bookmark name.
3. **Remove All** will delete all bookmarks in the window.

The **Find** window **Bookmark** tab will also appear when using functions other than **Find** such as when clicking on the Display All Bookmarks icon.

5.1.9 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the **Event Display**. The first selected byte appears on the third line of the display.

```
[CVEventDisplay]
SelectionOffset=2
```

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\User\Public\Public Documents\Frontline Test Equipment\)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

5.1.10 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.2 Bookmarks

Bookmarks are electronic sticky notes that you attach to frames of interest so they can be easily found later. In **Frame Display** bookmarked frames appear with a magenta triangle icon next to them.

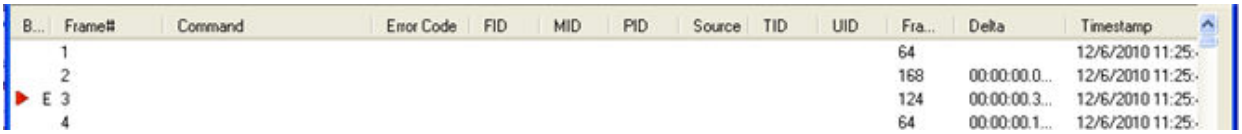
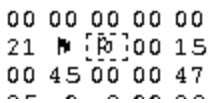


Figure 5.13 - Bookmarked Frame (3) in the Frame Display



In the **Event Display** bookmarks appear as a dashed line around the start of frame marker.

Bookmarks are easy to create and maintain, and are a very valuable tool for data analysis. When you create or modify a bookmark, you have up to 84 characters to explain a problem, leave yourself a reminder, leave someone else a reminder, etc. Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Once you have created a bookmark, you can use the Find function or other navigation methods to locate and move among them.

5.2.1 Adding, Modifying or Deleting a Bookmark

You can add, modify, or delete a bookmarks from **Frame Display** and **Event Display**

Add:

1. Select the frame or event you want to bookmark.
2. There are three ways to access the **Add Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**,
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Add Bookmark...**.
3. In the dialog box, add a comment (up to 84 characters) in the text box to identify the bookmark.
4. Click **OK**.

Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Modify

1. Select the frame or event with the bookmark to be edited.
2. There are three ways to access the **Add/Modfy Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**'
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Modify Bookmark...** on the selection.
3. Change the comment in the dialog box
4. Click **OK**. The edited bookmark will be saved as a part of the .cfa file.
5. You can also select **Display All Bookmarks** from the **Frame Display** and **Event Display** toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark you want to modify and click the **Modify...** button. Change the comment in the dialog box, and click **OK**.

Delete

1. Select the frame or event with the bookmark to be deleted.
2. There are three ways to access the **Add/Modfy Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**,
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Modify Bookmark...** on the selection.
3. Click on the **Delete** button. The bookmark will be deleted.
4. You can also select **Display All Bookmarks** from the **Frame Display** and **Event Display** toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark you want to delete and click the **Delete** button.

5.2.2 Displaying All and Moving Between Bookmarks

There are three ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Select Go to Next Bookmark from the Bookmarks menu.
3. Click the Display All Bookmarks icon . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.

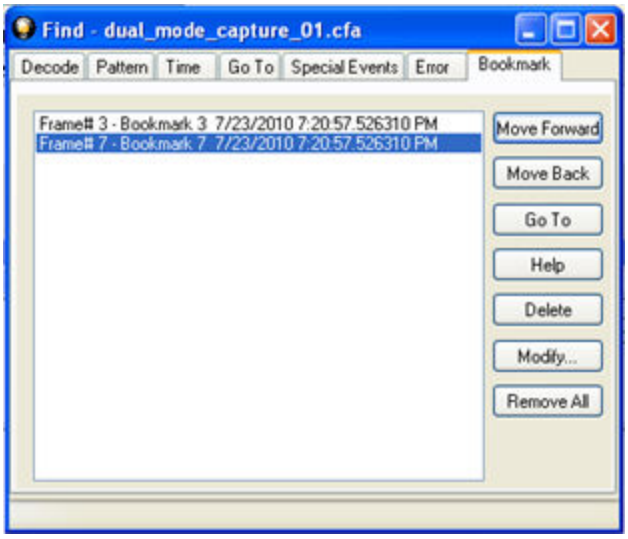


Figure 5.14 - Find Window Bookmark tab Used to Move Around With Bookmarks

To delete a bookmark, select it and click the **Delete** button.

To modify a bookmark, select it and click the **Modify** button.

Click **Remove All** to delete all the bookmarks.

Chapter 6 Saving and Importing Data

6.1 Saving Your Data

You can save all or part of the data that you have captured. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

On the **Control** window toolbar you can set up to capture a single file. Click here to see those settings.

There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data to disk.

6.1.1 Saving the Entire Capture File

This option is only available when you select **Single File** from the **Capture Mode** on **System Settings.** Click here to learn more about selecting Save options from System Settings.

1. If you are capturing data, click on the **Stop Capture** icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the **Event Display** or **Frame Display** window.
3. Click the **Save** icon, or select **Save** from the **File** menu.

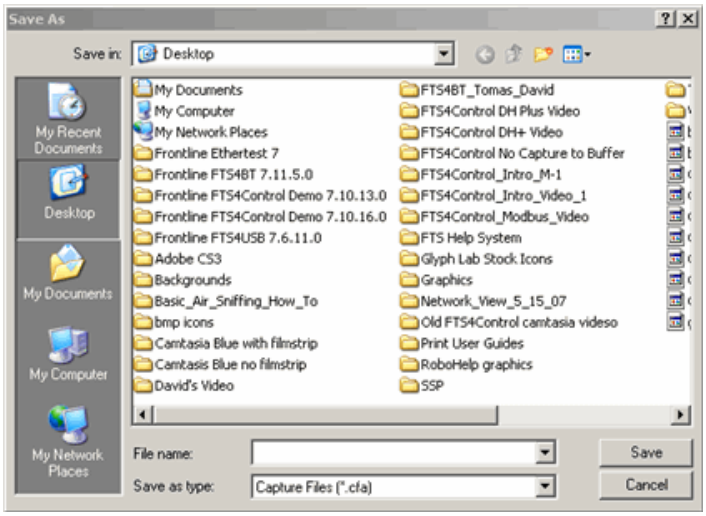
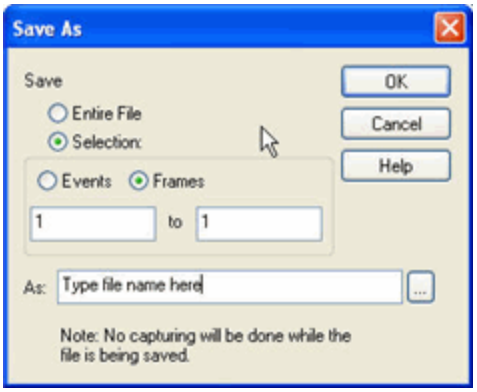


Figure 6.1 - Windows Save dialog

4. Type a file name in the **File name** box at the bottom of the screen.
5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.
6. When you are finished, click **OK**.

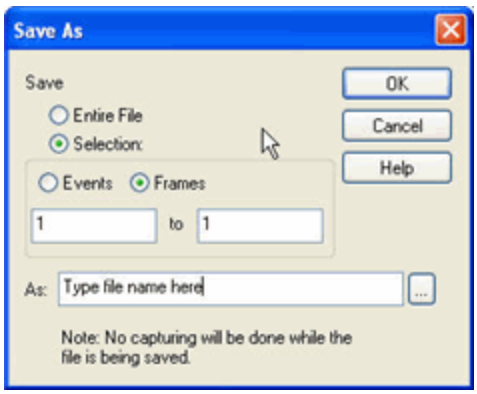
6.1.2 Saving the Entire Capture File with Save Selection

1. If you are capturing data, click on the **Stop** icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the **Event Display** or **Frame Display** window.
3. Right click in the data
4. Select **Save Selection** or **Save As** from the right click menu.
5. Click on the radio button labeled **Entire File**.
6. Choose to save **Events** or **Frames** . Choosing to save **Events** saves the entire contents of the capture file. Choosing to save **Frames** does not save all events in the capture file.
7. Type a file name in the **As** box at the bottom of the screen. Click the **Browse** icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
8. When you are finished, click **OK**.



6.1.3 Saving a Portion of a Capture File

1. If you are capturing data, click on the **Stop** icon to pause data capture. You cannot save data to a file while it is being captured.
2. Open the **Event Display** or **Frame Display** window, depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the **Frame Display** toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Right click in the data
5. Select **Save Selection** or **Save As** from the right click menu
6. Click on the radio button labeled **Selection**. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.
7. Select either **Events** or **Frames** to indicate whether the numbers are event or frame numbers.
8. Type a file name in the **As** box at the bottom of the screen. Click the **Browse** icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
9. Click **OK** when you are finished.



6.2 Adding Comments to a Capture File

The **Notes** feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the **Notes** window :

1. Click the **Show Notes** icon . This icon is present on the toolbars of the **Frame Display** , as well as the **Event Display** . **Notes** can be selected from the **Edit** menu on one of these windows.

2. Type your comments in the large edit box on the **Notes** window. The **Cut**, **Copy**, **Paste** features are supported from **Edit** menu and the toolbar when text is selected. Undo and Redo features are all supported from **Edit** menu and the toolbar at the current cursor location.
3. Click the thumbtack icon to keep the **Notes** window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

6.3 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- **Save To This File** – Saves the changes you have made to the current capture file.
- **Save As** – Saves the changes to a new file.
- **Cancel the Close Operation** – Closes the file and returns you back to the display. No changes are saved.
- **Discard Changes** – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

6.4 Loading and Importing a Capture File

6.4.1 Loading a Capture File

From the Control Window:

1. Go to the **File** menu.
2. Choose a file from the recently used file list.
3. If the file is not in the **File** menu list, select **Open Capture File** from the **File** menu or simply click on the **Open** icon on the toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click **Open**.

6.4.2 Importing Capture Files

1. From the **Control** window , go to the **File** menu and select Open Capture File or click on the Open icon on the toolbar.
2. Left of the **File name** text box, select from the drop-down list **Supported File Types** box to All Importable File Types or **All Supported File Types (*.cfa, *.log, *.txt, *.csv, *.cap)**. Select the file and click **Open**.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

6.5 Printing

6.5.1 Printing from the Frame Display/HTML Export

The **Frame Display Print** dialog and the **Frame Display HTML Export** are very similar. This topic discusses both dialogs.

Frame Display Print

The **Frame Display Print** feature provides the user with the option to print the capture buffer or the current selection. The maximum file size, however, that can be exported is 1000 frames.

When **Print Preview** is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images.

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select “Internet Options…” menu entry.
3. Click Advanced tab.
4. Check “Print background colors and images” under the Printing section
5. Click the Apply button, then click OK

Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to Selection and allows the user to choose the All radio button. When only one frame is selected, the All radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select **Print** or **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want access to printer options.

2. Choose to include the **Summary** pane (check the box) in the print output. The **Summary** pane appears at the beginning of the printed output in tabular format. If you select **All layers** in the **Detail Section**, the **Data Bytes** option becomes available.

3. In the **Detail Section**, choose to exclude—**No decode section**—the decode from the **Detail** pane in the **Frame Display**, or include **All Layers** or **Selected Layers Only.** If you choose to include selected layers, then select (click on and highlight) the layers from the list box.

4. Click on selected layers in the list to de-select, or click the **Reset Selected Layers** button to de-select all selected layers.

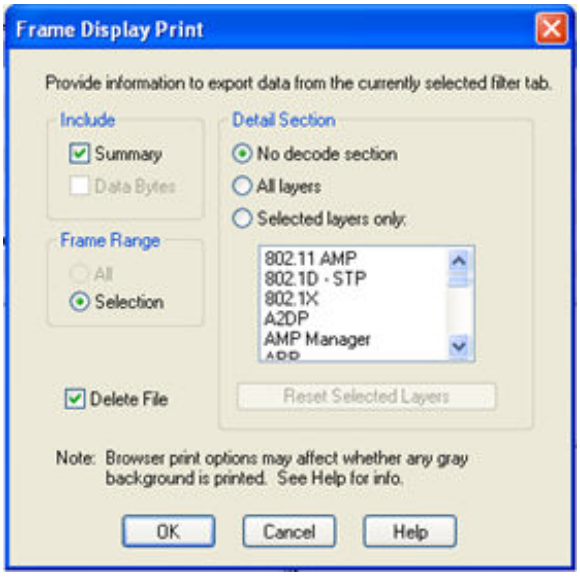


Figure 6.2 - Frame Display Print Dialog

5. Select the range of frames to include **All** or **Selection** in the **Frame Range** section of the **Frame Display Print** dialog.

   Choosing **All** prints up to 1000 frames from the buffer.

   Choosing **Selection** prints only the frames you select in the Frame Display window.

6. Selecting the **Delete File** deletes the temporary html file that was used during printing

7. Click the **OK** button.

Frame Display Print Preview

The **Frame Display Print Preview** feature provides the user with the option to export the capture buffer to an .html file. The maximum file size, however, that can be exported is 1000 frames.

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

1. Select **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print Preview**.

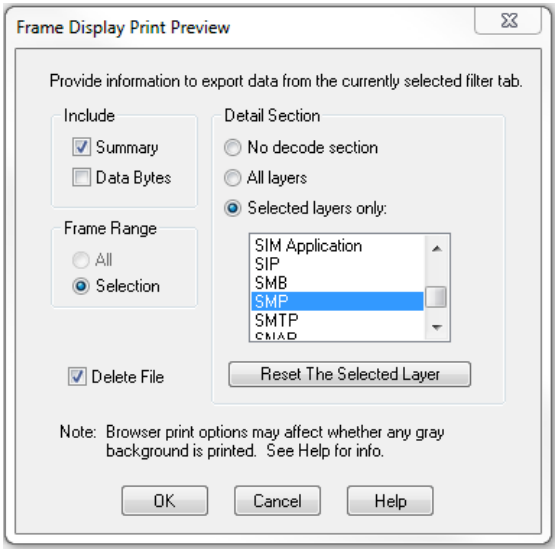


Figure 6.3 - Frame Display Print Preview Dialog

2. From this point the procedure is the same as steps 2 through 5 in "How to Print Frame Display Data" above.
3. Click the **OK** button, and after a brief wait a browser window will appear.

6.5.2 Printing from the Event Display

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When Print Preview is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select “Internet Options…” menu entry.
3. Click Advanced tab.
4. Check “Print background colors and images” under the Printing section
5. Click the Apply button, then click OK

The **Event Display Print** feature uses the current format of the **Event Display** as specified by the user.

See About Event Display for an explanation on formatting the **Event Display** prior to initiating the print feature.

Configure the Print File Range in the Event Display Print dialog

Selecting more than one event in the **Event Display** window defaults the radio button in the **Event Display Print** dialog to **Selection** and allows the user to choose the **All** radio button. When only one event is selected , the **All** radio button in the **Event Display Print** dialog is selected.

How to Print Event Display Data to a Browser

1. Select **Print** or **Print Preview** from the **File** menu on the **Event Display** window to display the **Event Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want preview the print in your browser.
2. Select the range of events to include from either **All** or **Selection** in the **Event Range** section . Choosing **All** prints all of the events in the capture file or buffer. Choosing **Selection** prints only the selected events in the Event Display window.

Note: In order to prevent a Print crash, you cannot select **All** if there are more than 100,000 events in the capture buffer.

Note: See "Configure the Print File Range in the Event Display Print Dialog" above for an explanation of these selections

Figure 6.4 - Event Display Print Dialog

3. Click the OK button.

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

6.6 Exporting

6.6.1 Frame Display Export

You can dump the contents of the **Summary** pane on the **Frame Display** into a Comma Separated File (.csv).

To access this feature:

1. Right click on the **Summary** pane or open the **Frame Display File** menu.
2. Select the **Export…** menu item.
3. Select a storage location and enter a **File name**.
4. Select **Save**.

6.6.2 Exporting a File with Event Display Export

With the **Event Display Export** dialog you can export the contents of the **Event Display** dialog as a test (.txt), CSV (.csv.), HTML (.htm), or Binary File (.bin). You also have the option of exporting the entire capture buffer or just the current selection of the Event Display dialog.

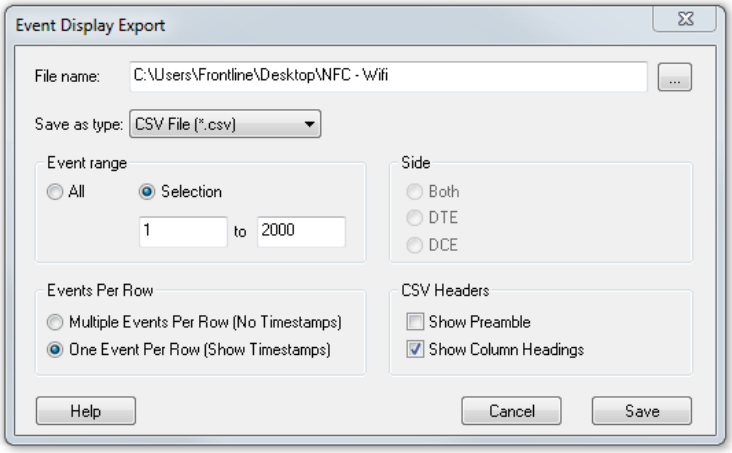


Figure 6.5 - Event Display Export Example: .csv file.

How to Export Event Display Data to a File

1. Select **Export Events** from the **File** menu on the **Event Display** window to display the **Event Display Export** dialog.
2. Enter a file path and name, or click the browser button to display the Windows **Save As** dialog and navigate to the desired storage location.
3. Select a file type from the **Save as type:** drop-down List Menu on the Event Display Export dialog. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)
4. Select the range of events to include in the file from either **All** or **Selection** in the **Event Range** section of the **Event Display Export** dialog.

- Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.
- When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.

5. Next you need to select the Side variable for serial communications.
   - is used to determine whether you want to export data from , or both.
   - Choose Host, Function\Control or Both to determine how you want to export the data.
5. Choose Host, Function\Control or Both to determine how you want to export the data.
6. Choose whether you want to display multiple events or single events per row.

   Events Per Row: You can choose to display **Multiple Events Per Row**, but this method contains no timestamps. If you select **One Event Per Row**, you can display timestamps. multiple events or single events per row.

   Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

   .

   The timestamp data types displayed in columns for One Event Per Row.

   Timestamp

   Delta

   Event Number

   Byte Number

   Frame Number

   Type

   Hex

   Dec

   Oct

   Bin

   Side

   ASCII | 7-bit ASCII | EBCDIC | Baudot

   RTS

   CTS

   DSR

   DTR

CD

RI

UART Overrun

Parity Error

Framing Error

7. If you select .csv as the file type, choose whether you want to hide/display **Preambles** or **Column Headings** in the exported file
8. Click **Save**. The Event Display Export file is saved to the locations you specified in **File name**.

	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	Delta	Event Number	Byte Number	Frame Number	Type	Hex	Dec	Oct	Bin	ASCII
632	11/30/2012 12:20:02.895166 PM	0:00:00.00	631	626	3	Data	0	0	0	0	.
633	11/30/2012 12:20:02.895166 PM	0:00:00.00	632	627	3	Data	0	0	0	0	.
634	11/30/2012 12:20:02.895166 PM	0:00:00.00	633	628	3	Data	0	0	0	0	.
635	11/30/2012 12:20:02.895166 PM	0:00:00.00	634	629	3	Data	98	152	230	10011000	.
636	11/30/2012 12:20:02.895166 PM	0:00:00.00	635	630	3	Data	70	112	160	1110000	p
637	11/30/2012 12:20:02.895166 PM	0:00:00.00	636	631	3	Data	94	148	224	10010100	.
638	11/30/2012 12:20:02.895166 PM	0:00:00.00	637	632	3	Data	22	34	42	100010	"
639	11/30/2012 12:20:02.895166 PM	0:00:00.00	638	633	3	Data	21	33	41	100001	!
640	11/30/2012 12:20:02.895166 PM	0:00:00.00	639	634	3	Data	1c	28	34	11100	.
641	11/30/2012 12:20:02.895166 PM	0:00:00.00	640	635	3	Data	80	128	200	10000000	.
642	11/30/2012 12:20:02.895166 PM	0:00:00.00	641	636	3	Data	80	128	200	10000000	.
643	11/30/2012 12:20:02.895166 PM	0:00:00.00	642	637	3	Data	80	128	200	10000000	.
644	11/30/2012 12:20:02.895166 PM	0:00:00.00	643	638	3	Data	80	128	200	10000000	.

Figure 6.6 - Example: .csv Event Display Export, Excel spreadsheet

6.6.2.1 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the **Filter Out** box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

6.6.2.2 Exporting Baudot

When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

Chapter 7 General Information

7.1 System Settings and Progam Options

7.1.1 System Settings

Open the **System Settings** window by choosing **System Settings** from the **Options** menu on the **Control** window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.

Single File

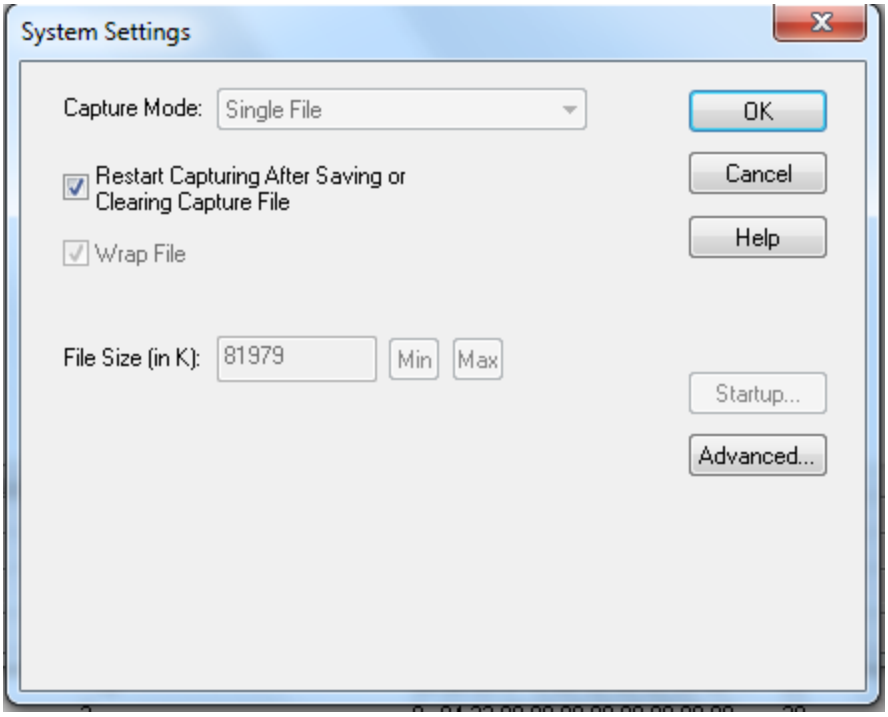


Figure 7.1 - System Settings Single File Mode

This option allows the analyzer to capture data to a file. Each time you capture the file you must provide a file name. The size of each file cannot larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

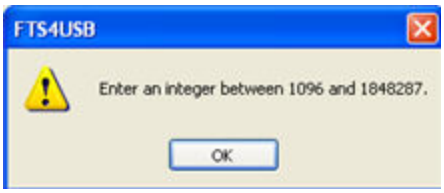
- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size**: The size of the file will depend of the available hard disk space.

  1. Click the **Min** button to see/set the minimum acceptable value for the file size.

  2. Click the **Max** button to see/set the maximum acceptable value for the file size.



You can accept these values, or you can enter a unique file size. But if you try to close the dialog after entering a value greater than the maximum or less than the minimum, you will see the following dialog.

- **Start up**

  Opens the Program Start up Options window. **Start up** options let you choose whether to start data capture immediately on opening the analyzer.

- **Advanced**

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

7.1.1.1 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the **System Settings** dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the **Startup** options and **Advanced** system options on the **System Settings** dialog and make changes to the settings at any time.

7.1.1.2 Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control window.
2. Choose **System Settings** from the **Options** menu.
3. On the **System Settings** window, click the **Advanced** button.

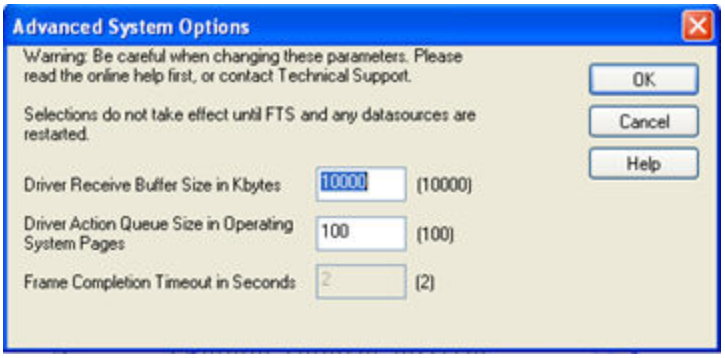

Advanced System Options
Warning: Be careful when changing these parameters. Please read the online help first, or contact Technical Support.
Selections do not take effect until FTS and any datasources are restarted.
OK
Cancel
Help
Driver Receive Buffer Size in Kbytes
10000
(10000)
Driver Action Queue Size in Operating System Pages
100
(100)
Frame Completion Timeout in Seconds
2
(2)

Figure 7.2 - Advanced System Options dialog

- **Driver Receive Buffer Size in Kbytes** - This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.
- **Driver Action Queue Size In Operating System Pages** - This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.
- **Frame Completion Timeout in Seconds** - This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

  If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

Note: This option is currently disabled.

7.1.1.3 Selecting Start Up Options

To open this window:

1. Choose **System Settings** from the **Options** menu on the Control window.
2. On the System Settings window, click the **Start Up** button.
3. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

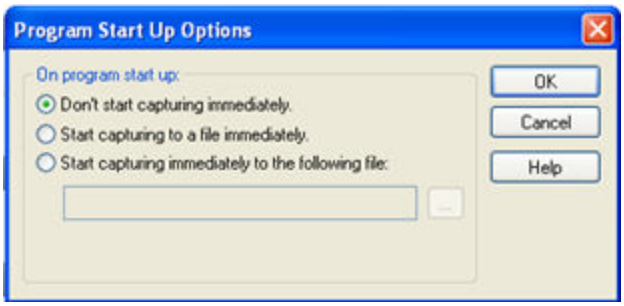


Figure 7.3 - Start Up Options dialog

- **Don't start capturing immediately** - This is the default setting. The analyzer begins monitoring data but does not begin capturing data until clicking the **Start Capture** icon on the **Control**, **Event Display** or **Frame Display** windows.
- **Start capturing to a file immediately** - When the analyzer starts up, it immediately opens a capture file and begins data capture to it. This is the equivalent of clicking the**Start Capture** icon. The file is given a name based on the settings for capturing to a file or series of files in the **System Settings** window.
- **Start capturing immediately to the following file:** - Enter a file name in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

7.1.2 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose **Directories** from the **Options** menu on the **Control** window to open the **File Locations** window.

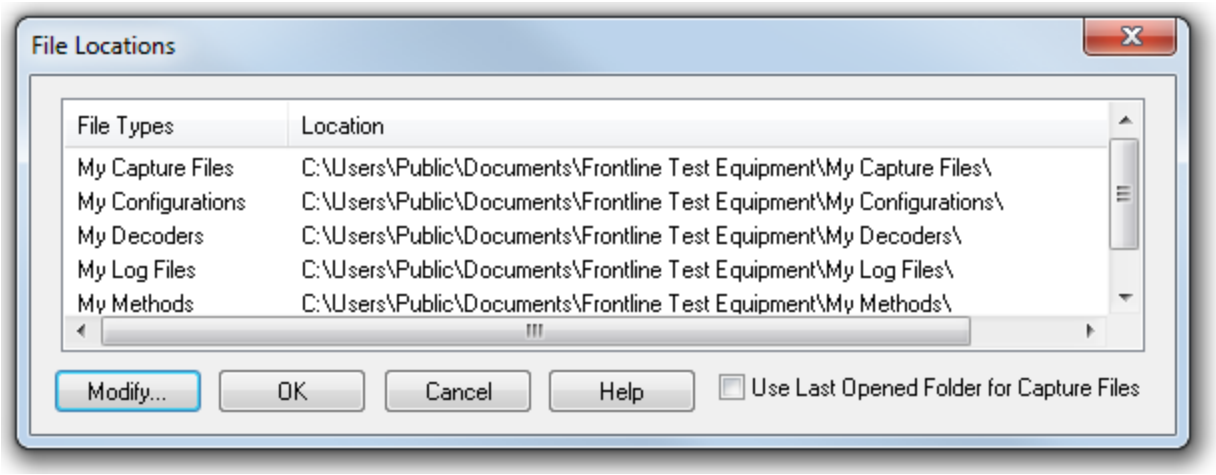


Figure 7.4 - File Locations dialog

2. Select the default location you wish to change.
3. Click **Modify**.
4. Browse to a new location.

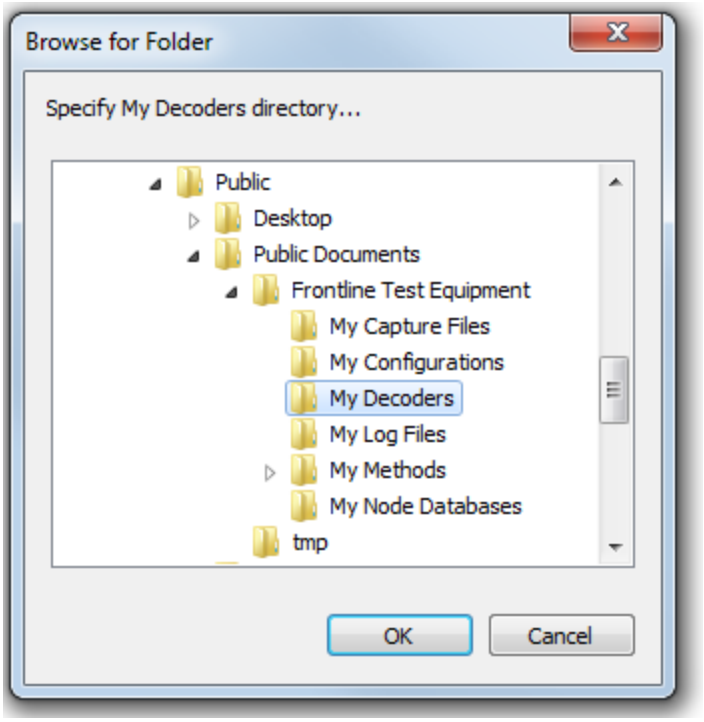


Figure 7.5 - File Locations Browse dialog

5. Click **OK**.
6. Click **OK** when finished.

If a user sets the My Decoders directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch Frontline. For example, if an Frontline product is installed at C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\ then "My Decoders" cannot be set to any of the following:

- C:\ My Decoders\
- C:\Users\ My Decoders\
- C:\Users\\Public\My Decoders\
- C:\Users\Public\Public Documents\My Decoders\
- or to any directory that already exists in the path C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\

Default Capture File Folder Checkbox

If the **Use Last Opened Folder for Capture Files** checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the default location for saving capture files is Drive A > Folder A. Now you select the **Use Last Opened Folder for Capture Files** checkbox. The next time, however, you open a capture file from a different location, Folder B > Removable Flash Drive for example. Now when you save the capture file, it will be saved to Folder B > Removable Flash Drive. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

There is one caveat to this scenario, however. Let's say you have selected **Use Last Opened Folder for Capture Files** and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. **ComProbe software will always try to save a file to the folder where the last file was opened from or saved to, if Use Last Opened Folder for Capture Files is checked.** If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

7.1.3 Side Names

The **Side Names** dialog is used to change the names of objects and events that appear in various displays. **The Side Names** dialog will change depending on the sniffing technology in use at the time the software was loaded.

Changes to the Names are used throughout the program.

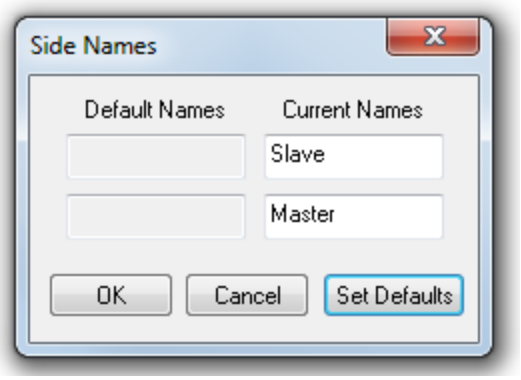


Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current

1. To open the Side Names dialog, choose **Side Names...** from the **Options** menu on the **Control** window.
2. To change a name, click on the name given in the **Current Names** column, and then click again to modify the name (a slow double-click).
3. Select **OK** to initiate the changes. The changes that have been made will not fully take effect for any views already open. Closing and reopening the views will cause the name change to take effect.
4. To restore the default values, click the **Set Defaults** button.

7.1.4 Timestamping

Timestamping is the process of precise recording in time of packet arrival. Timestamps is an optional parameter in the Frame Display and Event Display that can assist in troubleshooting a network link.

7.1.4.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

Choose **Set Timestamp Format...** from the **Options** menu on the Frame Display and Event Display window or click on the **Timestamping Option** icon in the **Event Display** toolbar. The Timestamping Options window will open.

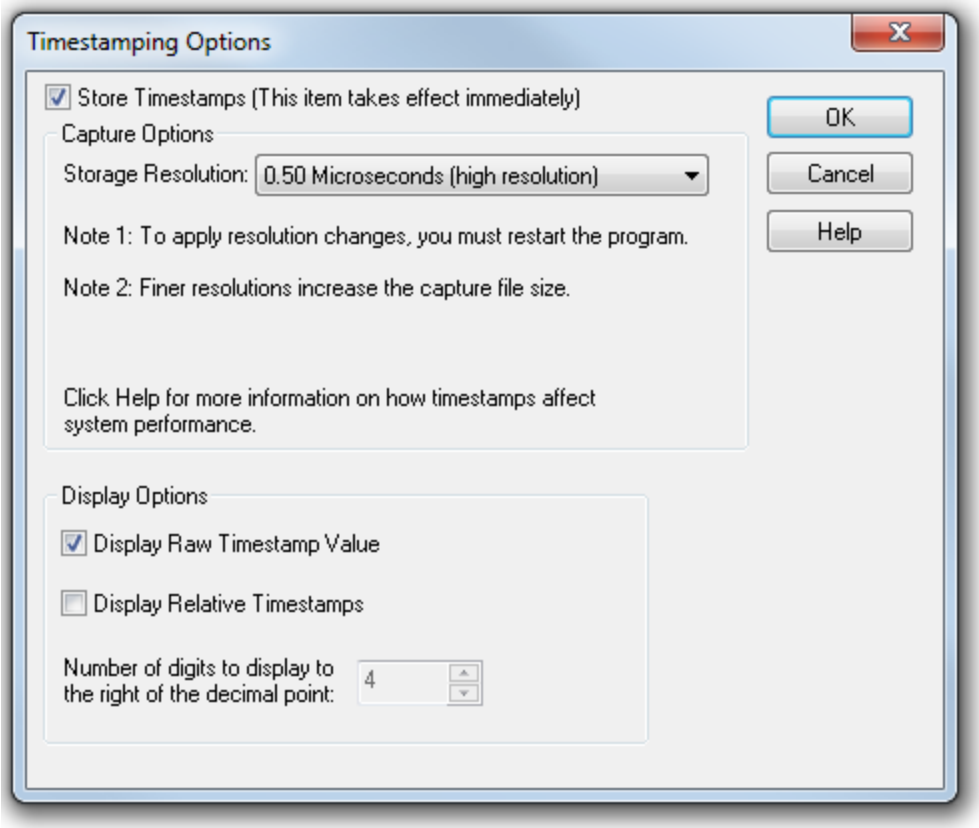

Timestamping Options
Store Timestamps (This item takes effect immediately)
Capture Options
Storage Resolution: 0.50 Microseconds (high resolution)
Note 1: To apply resolution changes, you must restart the program.
Note 2: Finer resolutions increase the capture file size.
Click Help for more information on how timestamps affect system performance.
Display Options
Display Raw Timestamp Value
Display Relative Timestamps
Number of digits to display to the right of the decimal point: 4
OK
Cancel
Help

Figure 7.1 Timestamping Options dialog

7.1.4.2 Enabling/Disabling Timestamp

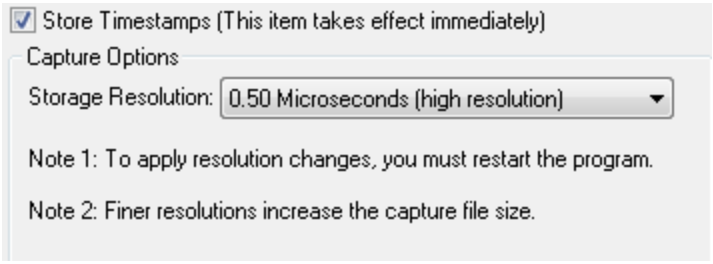
To enable timestamping click to make a check appear in the check box **Store Timestamps (This time takes effect immediately)**. Removing the check will disable timestamping.

7.1.4.3 Changing the Timestamp Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:


Store Timestamps (This item takes effect immediately)
Capture Options
Storage Resolution: 0.50 Microseconds (high resolution)
Note 1: To apply resolution changes, you must restart the program.
Note 2: Finer resolutions increase the capture file size.

1. Go to the **Capture Options** section of the window.
2. Change the resolution listed in the **Storage Resolution** box.

Note: If you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

7.1.4.3.1 Performance Issues with High Resolution Timestamp

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

7.1.4.4 Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window and find the **Display Relative Timestamps** checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Note: The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- **Display Raw Timestamp Value** shows the timestamp as the total time in hundred nanoseconds from a specific point in time.
- **Display Relative Timestamps** shows the timestamp as the amount of time that has passed since the first byte was captured. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.
- Selecting both values displays the total time in nanoseconds from the start of the capture as opposed to a specific point in time.
- Selecting neither value displays the actual chronological time.

When you select **Display Relative Timestamp** you can set the number of digits to display using the up or down arrows on the numeric list.

7.1.4.5 Displaying Fractions of a Second

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window, and find the **Number of Digits to Display** box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

7.2 Technical Information

7.2.1 Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Buffer overflow errors are an indicator that the analyzer is unable to keep up with the data. The information below describes what happens to the data as it arrives, what the error means, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

The analyzer's driver takes data from the driver and counts each byte as they are put into the driver's buffer. The analyzer's driver tells the user interface that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

Driver Buffer Overflows occur when the user interface does not retrieve frames from the driver quickly enough. Buffer overflows are indicated in the **Event Display** window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost.

There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by the analyzer. (Ethernet Only)
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the **Event Display** window or other processor intensive activities while the analyzer is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the file. Try turning off timestamping from the Timestamping Options window.
- For **Driver Buffer Overflows**, change the size of the driver buffer. This value is changed from the **Advanced System Settings**. Go to the **Control** window and choose **System Settings** from the **Options** menu. Click on the **Advanced** button. Find the value D**river Receive Buffer Size in Operating System Pages**. Take the number listed there and double it.
- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the **Event Display** and **Frame Display** windows. The analyzer can capture data with no windows other than the **Control** window open.

- If you are still experiencing buffer overflows after trying all of the above options, then you need to use a faster PC.

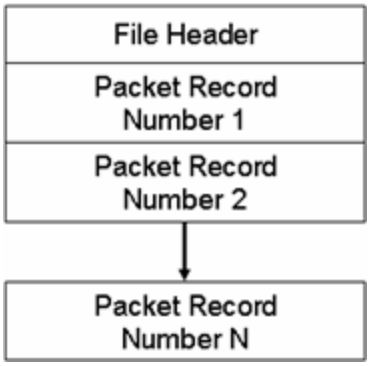
7.2.2 BTSnoop File Format

Overview

The BTSnoop file format is suitable for storing Bluetooth® HCI traffic. It closely resembles the snoop format, as documented in RFC 1761.

File Format

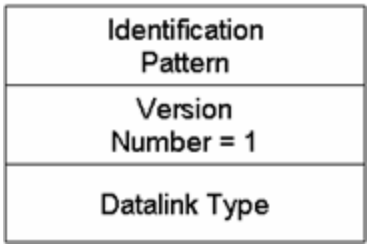
The snoop packet capture file is an array of octets structured as follows:



The File Header is a fixed-length field containing general information about the packet file and the format of the packet records it contains. One or more variable-length Packet Record fields follow the File Header field. Each Packet Record field holds the data of one captured packet.

File Header

The structure of the File Header is as follows:



Identification Pattern:

A 64-bit (8 octet) pattern used to identify the file as a snoop packet capture file. The Identification Pattern consists of the 8 hexadecimal octets:

62 74 73 6E 6F 6F 70 00

This is the ASCII string "btsnoop" followed by one null octets.

Version Number:

A 32-bit (4 octet) unsigned integer value representing the version of the packet capture file being used. This document describes version number 1.

Datalink Type:

A 32-bit (4 octet) field identifying the type of datalink header used in the packet records that follow. The datalink type codes are listed in the table below. Values 0 - 1000 are reserved, to maximize compatibility with the RFC1761 snoop version 2 format.

Table 7.2 - Datalink Codes

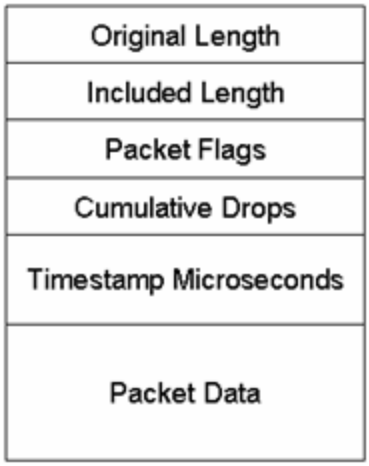
Datalink Type	Code
Reserved	0 - 1000
Un-encapsulated HCI (H1)	1001
HCI UART (H4)	1002
HCI BSCP	1003
HCI Serial (H5)	1004
Unassigned	1005 - 4294967295

Packet Record Format

Each packet record holds a partial or complete copy of one packet as well as some descriptive information about that packet. The packet may be truncated in order to limit the amount of data to be stored in the packet file.

Each packet record holds 24 octets of descriptive information about the packet, followed by the packet data, which is variable-length, and an optional pad field. The descriptive information is structured as six 32-bit (4-octet) integer values.

The structure of the packet record is as follows:



Original Length

A 32-bit unsigned integer representing the length in octets of the captured packet as received via a network.

Included Length

A 32-bit unsigned integer representing the length of the Packet Data field. This is the number of octets of the captured packet that are included in this packet record. If the received packet was truncated, the Included Length field is less than the Original Length field.

Packet Flags

Flags specific to this packet. Currently the following flags are defined:

Table 7.3 - Packet Flag Description

Bit No.	Definition
0	Direction flag 0 = Sent, 1 = Received
1	Command flag 0 = Data, 1 = Command/Event
2 - 31	Reserved

Bit 0 is the least significant bit of the 32-bit word.

Direction is relative to host / DTE. i.e. for Bluetooth controllers, Send is Host->Controller, Receive is Controller->Host.

Note: Some Datalink Types already encode some or all of this information within the Packet Data. With these Datalink Types, these flags should be treated as informational only, and the value in the Packet Data should take precedence.

Cumulative Drops

A 32-bit unsigned integer representing the number of packets that were lost by the system that created the packet file between the first packet record in the file and this one. Packets may be lost because of insufficient resources in the capturing system, or for other reasons.

Note: some implementations lack the ability to count dropped packets. Those implementations may set the cumulative drops value to zero.

Timestamp Microseconds

A 64-bit signed integer representing the time of packet arrival, in microseconds since midnight, January 1st, 0 AD nominal Gregorian.

In order to avoid leap-day ambiguity in calculations, note that an equivalent epoch may be used of midnight, January 1st 2000 AD, which is represented in this field as 0x00E03AB44A676000.

Packet Data

Variable-length field holding the packet that was captured, beginning with its datalink header. The Datalink Type field of the file header can be used to determine how to decode the datalink header. The length of the Packet Data field is given in the Included Length field.

Note that the length of this field in not necessarily rounded to any particular multi-octet boundary, as might otherwise be suggested by the diagram.

Data Format

All integer values are stored in "big-endian" order, with the high-order bits first.

7.2.3 Ring Indicator

The following information applies when operating the analyzer in **Spy** mode or **Source DTE, No FTS Cables** mode. When using the cables supplied with the analyzer to capture or source data, Ring Indicator (RI) is routed to a different pin which generates interrupts normally.

There is a special case involving Ring Indicator and computers with 8250 UARTs or UARTs from that family where the state of RI may not be captured accurately. Normally when a control signal changes state from high to low or low to high, an interrupt is generated by the UART, and the analyzer goes to see what has changed and record it.

Ring Indicator works a little differently. An interrupt is generated when RI changes from high to low, but not when RI changes from low to high. If Ring Indicator changes from low to high, the analyzer does not know that RI has changed state until another event occurs that generates an interrupt. This is simply the way the UART works, and is not a deficiency in the analyzer software.

To minimize the chance of missing a Ring Indicator change, the analyzer polls the UART every millisecond to see if RI has changed. It is still possible for the analyzer to miss a Ring Indicator change if RI and only RI changes state more than once per millisecond.

UARTs in the 8250 family include 8250s, 16450s, 16550s and 16550 variants. If you have any questions about the behavior of your UART and Ring Indicator, please contact technical support.

7.2.4 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

7.2.5 Event Numbering

This section provides information about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

When the analyzer captures an event, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are wrapped out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file use the same event numbers that your file does.

7.2.6 Useful Character Tables

7.2.6.1 ASCII Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

7.2.6.2 Baudot Codes

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

7.2.6.3 EBCDIC Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

7.2.6.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash

characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Table 7.4 - Communications Control Characters

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle

Table 7.4 - Communications Control Characters(continued)

Abbreviation	Control Character	Text
US	US	Unit Separator
VT	VT	Vertical Tabulation

7.2.7 The Frontline Serial Driver

ComProbe software uses custom versions of the standard Windows serial drivers in order to capture data. These drivers are usually installed during the routine product installation. However, if you need to install the serial driver after ComProbe software has already been installed, please refer to the instructions available in the Setup folder installed under Start | Programs | [Product Name and version #] | Setup | How to Install the FTS Serial Driver.

7.2.8 DecoderScript Overview

The DecoderScript™ Reference Manual and User Guide is delivered with each Frontline ComProbe® Protocol Analysis System installation package under Developer Tools. The manual is also available on-line at FTE.com.

The main purpose of this manual is to describe DecoderScript™, the language used in writing decoders. DecoderScript allows you to create new decoders or modify existing decoders to expand the functionality of your ComProbe protocol analyzer. DecoderScript displays protocol data, checks the values of fields, validates checksums, converts and combines field values for convenient presentation. Decoders can also be augmented with custom C++-coded functions, called "methods", to extend data formatting, validation, transformations, and so on.

A decoder defines field-by-field how a protocol message can be taken apart and displayed. The core of each "decoder" is a program that defines how the protocol data is broken up into fields and displayed in the Frame Display window of the analyzer software.

This manual provides instruction on how to create and use custom decoders. When reading the manual for the first time, we encourage you to read the chapters in sequence. The chapters are organized in such a way to introduce you to DecoderScript writing step- by- step.

Screenshots of the ComProbe protocol analyzer have been included in the manual to illustrate what you see on your own screen as you develop decoders. But you should be aware for various reasons, the examples may be slightly different from the ones that you create. The differences could be the result of configuration differences or because you are running a newer version of the program. Do not worry if an icon seems to be missing, a font is different, or even if the entire color scheme appears to have changed. The examples are still valid.

Examples of decoders, methods, and frame recognizers are included in this manual. You can cut and paste from these examples to create your own decoders.

A quick note here: Usually the pasted code appears the same as the original in your editor. Some editors, however, change the appearance of the text when it is pasted (something to do with whether it is ASCII or Unicode text). If you find that the pasted text does not appear the same as the original, you can transfer the code into a simple text editor like Notepad, save it as an ANSI (ASCII) file, then use it in your decoder.

These files are installed in the FTE directory of the system Common Files directory. The readme file in the root directory of the protocol analyzer installation contains a complete list of included files. Most files are located in My Decoders and My Methods.

We will be updating our web site with new and updated utilities, etc, on a regular basis and we urge decoder writers to check there occasionally.

7.2.9 *Bluetooth* low energy ATT Decoder Handle Mapping

Low energy device attributes contain a 16-bit address called the attribute handle. Each handle is associated with an attribute Universally Unique Identifier (UUID) that is 128-bits long. In the attribute database, the handle is unique while the UUID is not unique.

The ComProbe software detects and stores the relationships (mappings) between handle and UUID during the GATT discovery process. But sometimes, there is no GATT discovery process because

- The discovery has previously taken place and both devices stored the mappings and the discovery will not repeat at every subsequent connection.
- The developer owns both devices in the conversation and chose to ignore discovery because the mappings are known.
- The devices are in development and the code to perform the mappings has not been written yet.

The solution to this problem is to

1. define the mappings in a file and
2. then pre-loading the mapping using the ComProbe software.

Creating handle-UUID mapping file

Create a file named "ATT_Handle_UUID_Preload.ini' in the root directory of "C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\", but the file can be located anywhere.

Assume that you want to create a GATT service starting at handle 1.

Create a section in the ini file called

```
[Service Base Handles]
A=1
```

"A" will be your first service. Make the base handle equal to the handle of your service. You can use all upper and lower case letters so you can have up to 52 service handles.

Next add the following section.

```
[Advertiser Handles]
; Generic Access Profile (GAP)
A0 = 1800
A1 = 2803
A2 = 2a00
A3 = 2803
A4 = 2a01
A5 = 2803
A6 = 2a04
```

A few tings of note:

- In the code above, lines begging with a semi-colon are comments.
- If you want to change the base handle of the GAP service, change the "1" to some other number.
- If you want to comment out the entire service, comment out the base handle. If no "A" is defined, the software will ignore "A1", "A2" and so on.

7.3 Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://fte.com/support/supportrequest.aspx

Email: tech_support@fte.com

If you need to talk to a technical support representative about your ComProbe BPA 500 product, support is available between 9 am and 5 pm, U.S. Eastern Time zone, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Instructional Videos

Frontline provides a series of videos to assist the user and may answer your questions. These videos can be accessed at fte.com/support/videos.aspx. On this web page use the **Video Filters** sidebar to select instructional videos for your product.

Appendicies

Appendix A: Application Notes **246**

Appendix A: Application Notes

A.1 Getting the Android Link Key for Classic Decryption 248

A.2 Decrypting Encrypted Bluetooth®data with ComProbe BPA 600 254

A.3 Decrypting Encrypted Bluetooth® low energy 262

A.4 Bluetooth® low energy Security 272

A.5 Bluetooth Virtual Sniffing 278

A.1 Getting the Android Link Key for Classic Decryption

Bluetooth devices on an encrypted link share a common “link key” used to exchange encrypted data. For a *Bluetooth* sniffer, such as the ComProbe BPA 600, to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

Bluetooth devices using the Android operating system have a "developer" option that will provide the link key for Classic *Bluetooth* decryption. This procedure will use the developer options to obtain the Android HCI (Host Controller Interface) log that contains the link keys for all active links..

A.1.1 What You Need to Get the Android Link Key

The process applies to the Android 4.4 or later operating system.

- Android device with Bluetooth enabled and paired with another *Bluetooth* device.
- ComProbe Protocol Analysis System installed on your computer
- Android Debug Bridge (optional)

Note: Each Android device model can vary in screen organization, layout and format. The directions in this paper are based on known typical Android device. Refer to the manufacturer's manual,on-line help, or technical support for detailed information about your particular device.

A.1.2 Activating Developer options

The Android HCI log will contain the link key for an active *Bluetooth* link.

1. On the Android device go to **Settings**,
2. Select **About**.
3. In the About screen tap on **Build number** eight times. At some point you will see a notice similar to "You are now a developer!".

Note: On some devices the build information may be under one or more sub-screens below the About screen. Also the number of taps may vary; in most cases the screen will provide

status of your tap count.

4. Return to the **Settings** screen and you will see **Developer options**

A.1.3 Retrieving the HCI Log

Now that **Developer options** have been activated on the Android device, you can retrieve the HCI log.

1. On the Android device go to **Settings**.
2. Select **Developer options**.
3. Click to enable **Bluetooth HCI snoop logging.**
4. Return to the **Settings** screen and select **Developer options**.
5. In the **Developer options** screen select **Enable Bluetooth HCI snoop log**. The log file is now enabled.

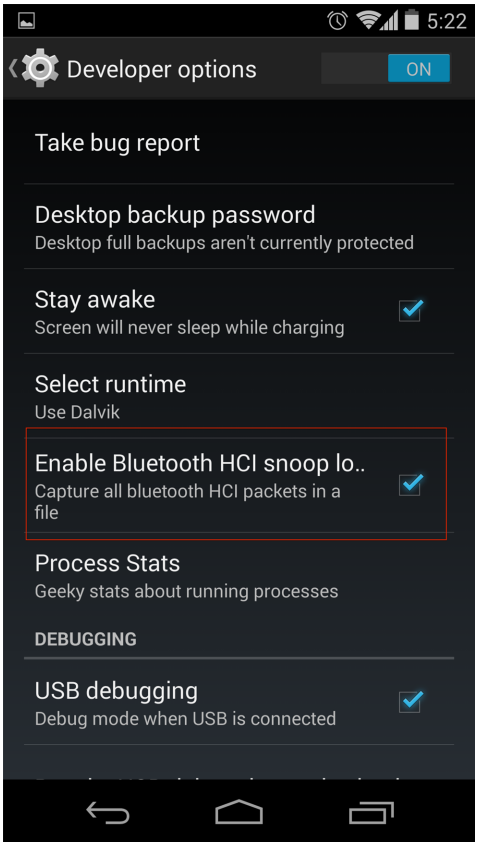


Figure 1 - Typical Android Developer options screen

6. On the Android device turn off *Bluetooth*.
7. Turn on *Bluetooth*.
8. Reboot the Android device.

The HCI log file is now being generated and is saved to */sdcard/btsnoop_hci.log*.

Note: Samsung devices have a slightly different location for the btsnoop file.

There are two options for retrieving the HCI log from the Android device.

a. Attach the Android device to your computer. The file */sdcard/btsnoop_hci.log* is in the root of one of the mountable drives. Copy the file to directory *C:/Users/Public/Public Documents/Frontline Test Equipement/My Capture File/*.

b. The second option is to use the Android Debug Bridge (ADB)using the following steps. The debug bridge is included with Android Software Developer Kit.

(1). On the Androd device **Development** screen, select **Android debugging** or **USB debugging**.

(2). Connect your computer and Android device with a USB cable.

(3). Open a terminal on your computer and run the following command.

```
adb devices.
```

(4). Your Android device should show up in this list confirming that ADB is working.

```
List of devices attached
XXXXXXXXXXX device
```

(5). In the terminal enter the following command to copy the HCI Log to your computer.

```
adb pull /sdcard/btsnoop_hci.log
```

A.1.4 Using the ComProbe Software to Get the Link Key

You will load the HCI Log file *btsnoop_HCI.log* into the ComProbe Protocol Analysis System on your computer as a capture file. Then you can use the **Frame Display** to locate the link key.

1. Activate the ComProbe Protocol Analysis System. (Refer to the ComProbe BPA 600 User Manual on fte.com).
2. From the Control window menu select **File**, **Open Capture File...**.
3. When the **Open** window appears, set the file type to **BTSnoop Files (*.log)**. If not already selected navigate to the *My Capture Files* directory and select *btsnoop_hci.log*.

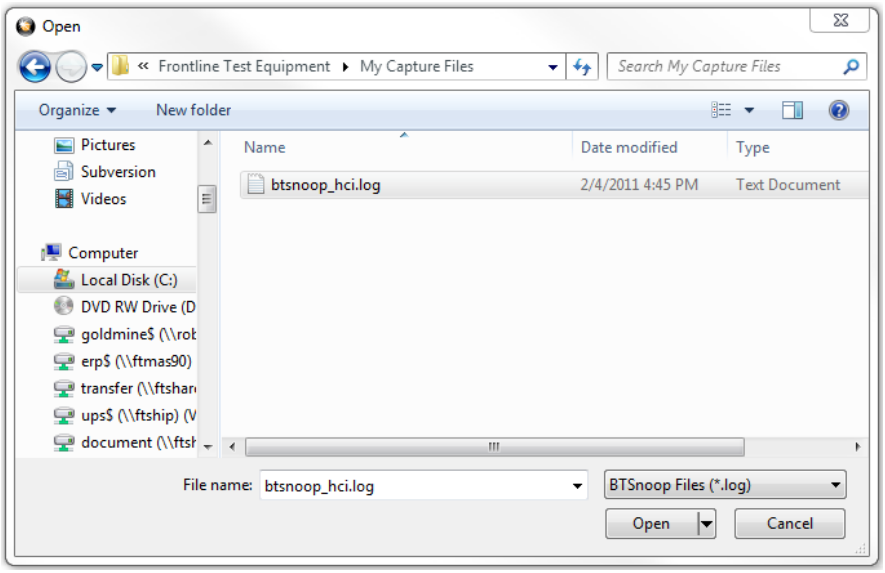


Figure 2 - Select Capture File

4. Open the **Frame Display**

5. In the **Frame Display** protocol tabs select **HCI**. (See image below)

6. Select Find , click on the **Decode** tab, and enter "link key" in the Search for String in Decode. Check the **Ignore Case** option. Click on **Find Next** until the Event column shows Link Key Notification.

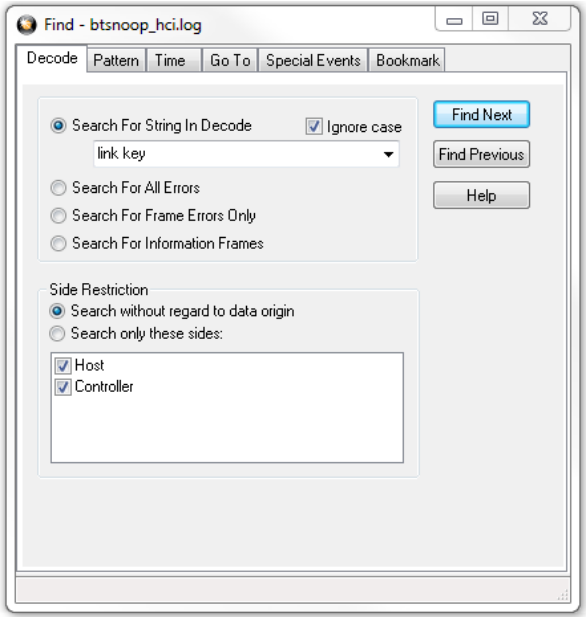


Figure 3 - Find Dialog

In the **Frame Display** Detail pane, expand HCI and HCI Event where the Link Key is shown. Copy and paste the Link Key into the appropriate BPA 600 datasource dialog. (See the example below)

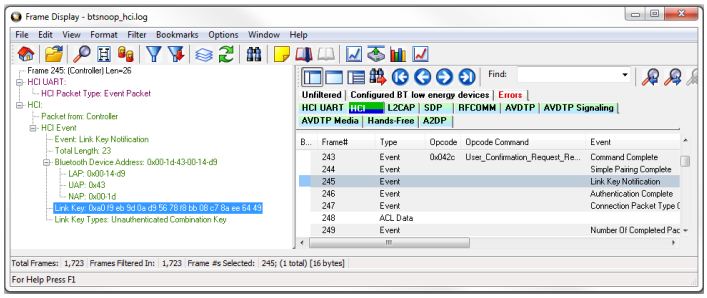

Frame Display - btsnoop_hci.log
File Edit View Format Filter Bookmarks Options Window Help
Frame 245: (Controller) Len=26
HCI UART:
HCI Packet Type: Event Packet
HCI:
Packet from: Controller
HCI Event
Event: Link Key Notification
Total Length: 23
Bluetooth Device Address: 0x00-1d-43-00-14-d9
LAP: 0x00-14-d9
UAP: 0x43
NAP: 0x00-1d
Link Key: 0xa0 f5 eb 9d 0a d9 56 78 f8 bb 08 c7 8a ee 64 43
Link Key Types: Unauthenticated Combination Key
Find:
Unfiltered | Configured BT low energy devices | Errors
HCI UART | HCI | L2CAP | SDP | RFCOMM | AVDTP | AVDTP Signaling
AVDTP Media | Hands-Free | A2DP
B... Frame# Type Opcode Opcode Command Event
243 Event 0x042c User_Confirmation_Request_Re... Command Complete
244 Event Simple Pairing Complete
245 Event Link Key Notification
246 Event Authentication Complete
247 Event Connection Packet Type
248 ACL Data
249 Event Number Of Completed Pac
Total Frames: 1,723 Frames Filtered In: 1,723 Frame #s Selected: 245; (1 total) [16 bytes]
For Help Press F1

Figure 4 - Frame Display Showing Link Key Notification Event with the Link Key

---

Author: John Trinkle with Joe Skupniewitz

Publish Date: 30 September 2014

A.2 Decrypting Encrypted Bluetooth®data with ComProbe BPA 600

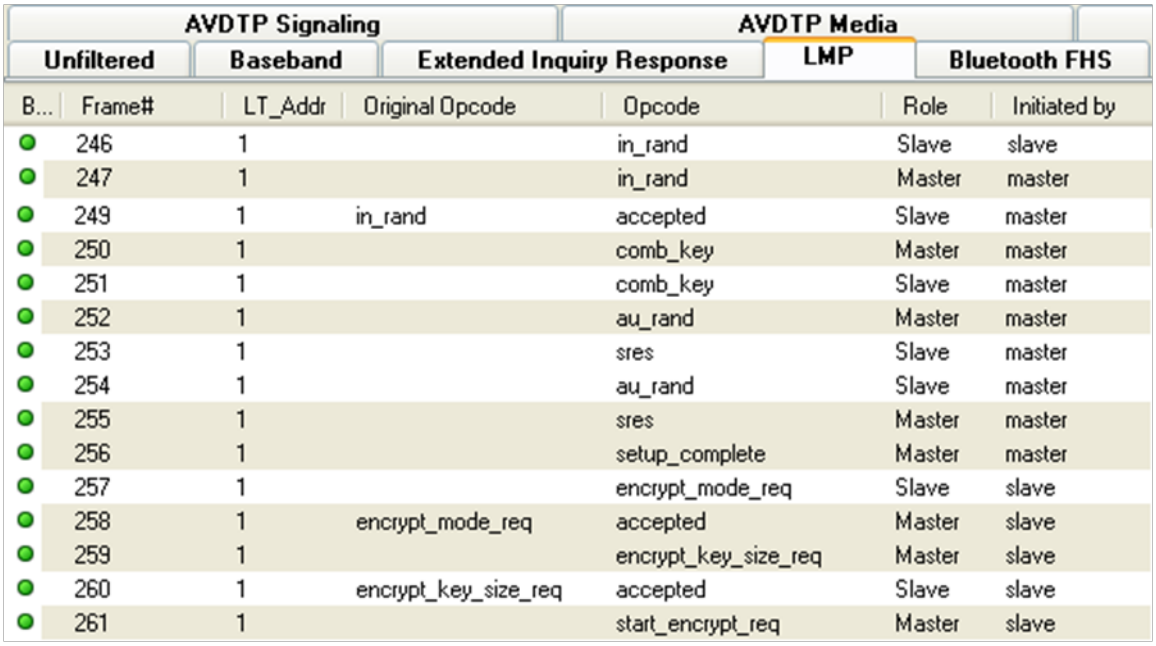
A.2.1 How Encryption Works in *Bluetooth*

Bluetooth devices on an encrypted link share a common "link key" used to exchange encrypted data. How that link key is created depends on the paring method. Paring methods have evolved and changed throughout *Bluetooth* history. The earlier legacy method was used up through *Bluetooth* 2.0. Improved and simpler pairing methods began with Bluetooth 2.1 and remain in the current version *Bluetooth* 4.0.

For a *Bluetooth* sniffer to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

A.2.2 Legacy Pairing (*Bluetooth* 2.0 and earlier)

In legacy pairing, this link key is derived from a shared PIN code, the master's *Bluetooth* clock, the master's BD_ ADDR and a random number that is passed between the two devices. If the sniffer has all of this same data, it can create the link key in the same way that the devices do. The sequence of events used to create this key, or pairing process, is shown in the ComProbe software Frame Display below.



AVDTP Signaling | AVDTP Media

Unfiltered | Baseband | Extended Inquiry Response | LMP | Bluetooth FHS

B...	Frame#	LT_Addr	Original Opcode	Opcode	Role	Initiated by
	246	1		in_rand	Slave	slave
	247	1		in_rand	Master	master
	249	1	in_rand	accepted	Slave	master
	250	1		comb_key	Master	master
	251	1		comb_key	Slave	master
	252	1		au_rand	Master	master
	253	1		sres	Slave	master
	254	1		au_rand	Slave	master
	255	1		sres	Master	master
	256	1		setup_complete	Master	master
	257	1		encrypt_mode_req	Slave	slave
	258	1	encrypt_mode_req	accepted	Master	slave
	259	1		encrypt_key_size_req	Master	slave
	260	1	encrypt_key_size_req	accepted	Slave	slave
	261	1		start_encrypt_req	Master	slave

Figure 5 - Frame Display

Frame 247 is the LMP_in_rand which is where a random number generated by the master is passed to the slave. The slave acknowledges that it has accepted the number in frame 249. The initialization key has been passed to the slave and is now shared by both devices. Both devices now independently generate combination keys.

In frames 250 and 251, the combination keys are passed between master and slave. In frame 252, the master sends its LMP_au_rand. This is the random number that has been encrypted using the link key that master has calculated. The slave then responds with frame 253, an LMP_sres confirming that it was able to compute the same number. That process is repeated in the other direction (slave to master) in frames 254 and 255. This completes the authentication between devices, and the setup_complete message is sent and the slave requests encryption mode in frame 257, and the master accepts in frame 258. The actual encryption starts after the start encryption request in frame 261.

In order for the ComProbe software to decrypt an encrypted *Bluetooth* conversation, the ComProbe software must compute the same link key being used by the devices being sniffed. Since this link key is never sent over the air, the ComProbe software must have all of the same information the devices being sniffed have so that it can calculate the same link key that each of the two devices does. To decrypt successfully, the ComProbe software must know the PIN code and capture:

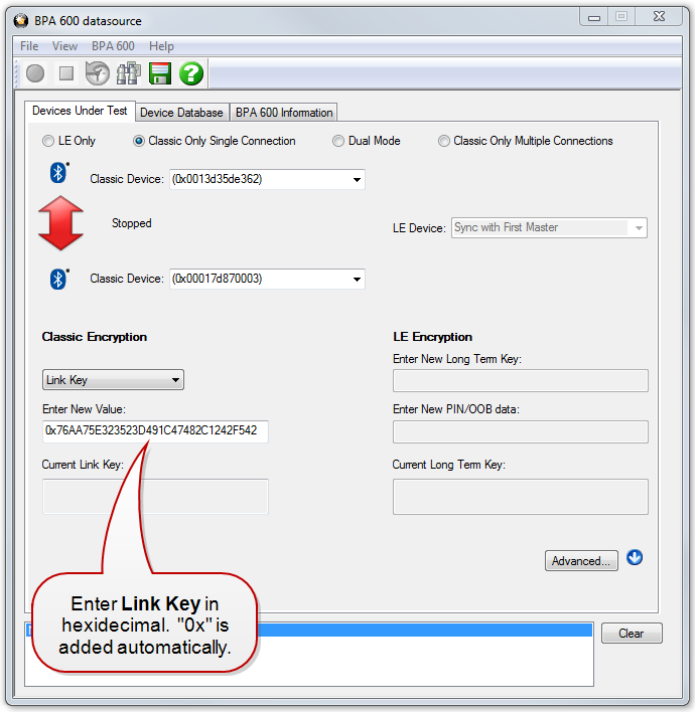
- The LMP_in_rand
- Both LMP_comb_keys
- Both LMP_au_rand/LMP_sres pairs.

If any of these are missed, the ComProbe software will not be able to decrypt. If you capture encrypted data and find that everything captured after the LMP_start_encryption_request is in error, look back at the LMP frames previous to that and you'll probably find one or more of these missing. The Start Encryption Request with also be marked by the ComProbe software with an error that indicates that the link key calculated by the ComProbe software is different from the one used by your devices.

A.2.3 Secure Simple Pairing (SSP) (Bluetooth 2.1 and later)

To capture and decrypt data between two *Bluetooth* devices using Secure Simple Pairing we have two choices. If one of your devices can be put into Secure Simple Pairing Debug Mode, all that needs to be done in I/O Settings is to choose your devices. It doesn't matter what's been selected in the Pairing Method drop down, the ComProbe software will see the debug messages being sent and calculate the correct key. Only one of the devices needs to be in debug mode and it doesn't matter which one.

If neither of your devices can be put into debug mode, you'll need to know the link key being used by one of your devices, generally by accessing the HCI on one of the devices. If that is the case, enter the link key into the box provided.



Note that the link key is sometimes stored in your device in reverse order. The ComProbe software will automatically reverse the link key, if needed.

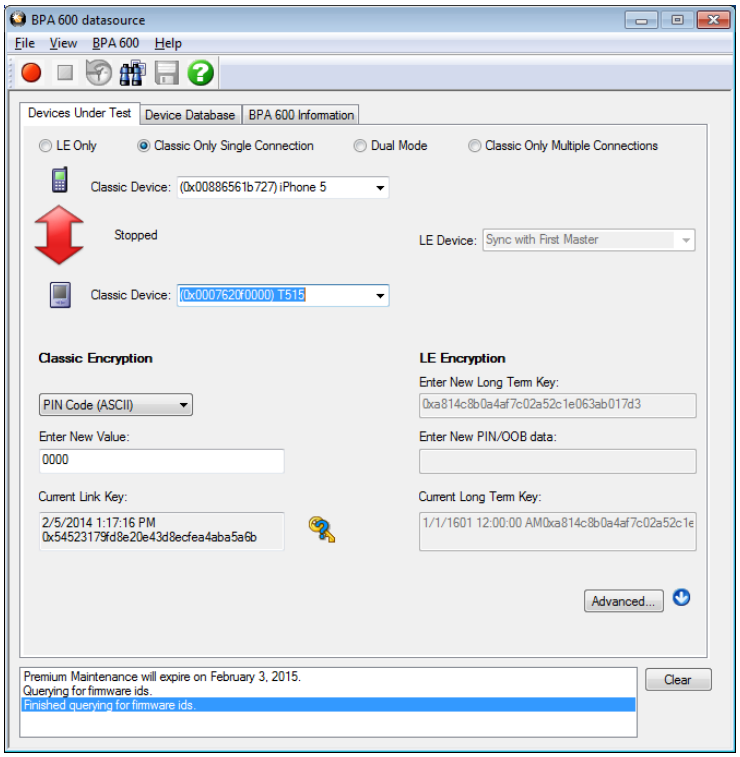
Once the link key has been entered, decryption operates the same way it does in legacy pairing.

A.2.4 How to Capture and Decrypt Data (Legacy Pairing)

Run the ComProbe software and select **Bluetooth Classic/low energy (BPA 600)**. This will open the **Control** window and the **BPA 600 Datasource** where ComProbe device parameters are set for sniffing including the devices to be sniffed and how the link key is to be encrypted.

Select the **Devices Under Test** tab. Make both your *Bluetooth* devices discoverable.

Click the **Discover Devices** on the datasource toolbar. The ComProbe software will find any discoverable *Bluetooth* devices within its range. You will then be able to select your devices from the drop down lists. If one or both of your devices cannot be made discoverable, you may type in the BD_ADDR(s) directly.



With legacy pairing, select **PIN Code (ASCII)** from the **Classic Encryption** drop down and fill in the PIN. As mentioned above, the ComProbe software needs the PIN code in order to calculate the link key the two *Bluetooth* devices are using. Alternately, you may enter the Link Key manually if it is known. The ComProbe software also keeps a database of the link keys it previously calculated, which may be accessed on the**Device Database** tab.

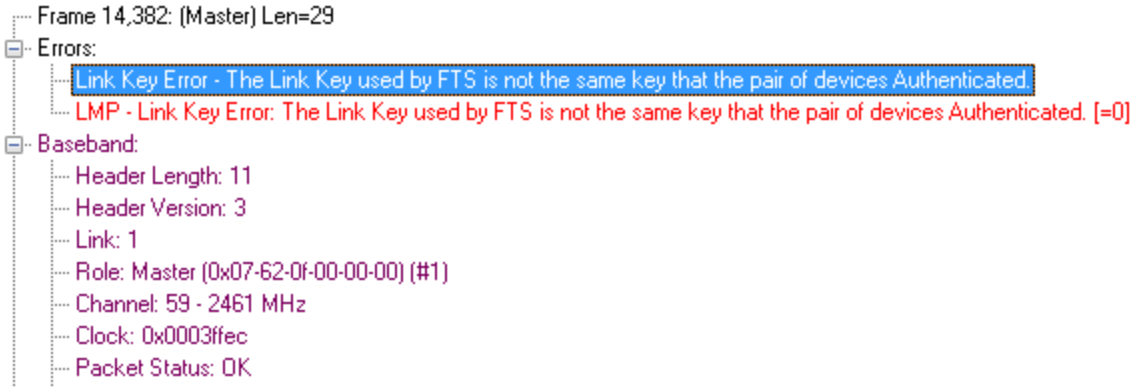
The **Start Sniffing** button should now be available. If Start Sniffing is grayed out, there is something set up incorrectly in the datasource **Device Under Test** tab. For example, if you selected PIN code in the encryption drop down but you neglected to fill in the PIN code, then Start Sniffing will be grayed out.

Click on the toolbar **Start Sniffing** button. The **Control** window will display a capture status message. When you start sniffing, the colored arrow be red indicating that the Bluetooth devices are initializing. . After a few seconds the arrow will turn green and the status will change to “Waiting for the master to connect to the slave”. At this point the BPA 600 is synchronized and waiting for a baseband connection.

When your connection is established, the arrow will turn blue , signifying that a baseband link has been established and data should start to appear in the **Frame Display**. The direction of the arrow indicates which device is master and which is slave. The arrow points from master to slave.

If ComProbe software successfully calculates the correct link key, the Link Key icon on the datasource is updated with a check mark to indicate that the link key has been verified. Should the link key be incorrect the link key icon will show .

An incorrect link key will show up in the **Frame Display**. Open the **Frame Display LMP** tab and search for frames with errors appearing in red. In the **Decode** pane a link key error will appear in red under **Errors**.


Frame 14,382: (Master) Len=29
Errors:
Link Key Error - The Link Key used by FTS is not the same key that the pair of devices Authenticated.
LMP - Link Key Error: The Link Key used by FTS is not the same key that the pair of devices Authenticated. [=0]
Baseband:
Header Length: 11
Header Version: 3
Link: 1
Role: Master (0x07-62-0f-00-00-00) (#1)
Channel: 59 - 2461 MHz
Clock: 0x0003ffec
Packet Status: OK

A.2.5 How to tell if a device is in Secure Simple Pairing Debug Mode

When a device is configured in SSP debug mode, the ComProbe software will decode and display the debug key in the Encapsulated Payload message of the **Frame Display Summary** pane. There will be an Encapsulated Payload message sent from both the master and the slave. The message from the device that is in debug mode will show the debug key, the other will show the public key. Refer to the **Frame Display Decode** pane in the screenshots below where the master is in SSP debug mode. Remember, only one of the *Bluetooth* devices needs to be in SSP debug mode.

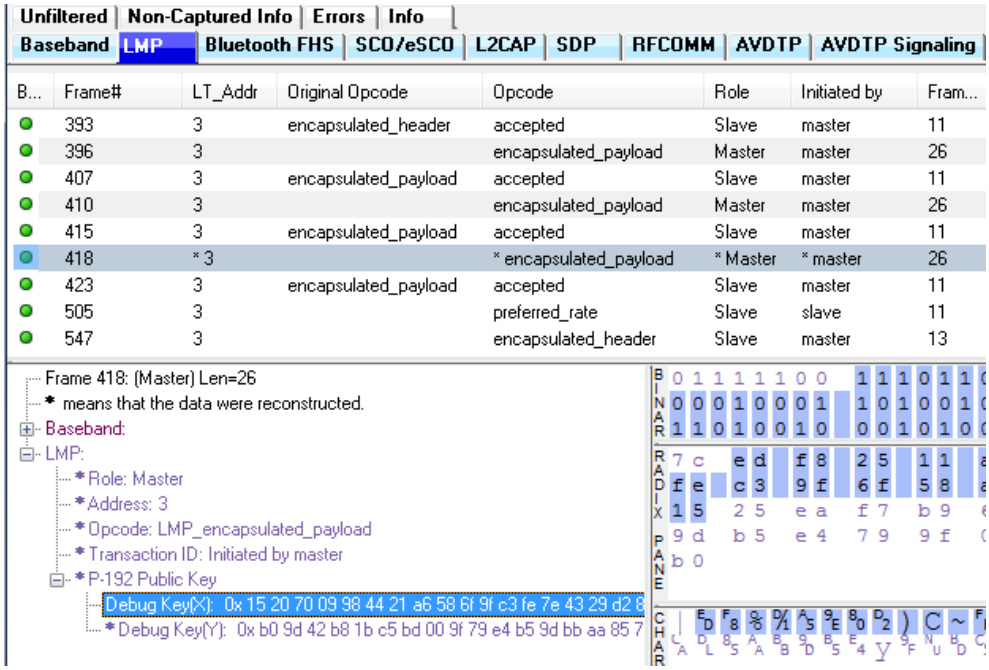

Unfiltered
Non-Captured Info
Errors
Info
Baseband
LMP
Bluetooth FHS
SCO/eSCO
L2CAP
SDP
RFCOMM
AVDTP
AVDTP Signaling
B... Frame# LT_Addr Original Opcode Opcode Role Initiated by Fram...
393 3 encapsulated_header accepted Slave master 11
396 3 encapsulated_payload Master master 26
407 3 encapsulated_payload accepted Slave master 11
410 3 encapsulated_payload Master master 26
415 3 encapsulated_payload accepted Slave master 11
418 * 3 * encapsulated_payload * Master * master 26
423 3 encapsulated_payload accepted Slave master 11
505 3 preferred_rate Slave slave 11
547 3 encapsulated_header Slave master 13
Frame 418: (Master) Len=26
* means that the data were reconstructed.
Baseband:
LMP:
*Role: Master
*Address: 3
*Opcode: LMP_encapsulated_payload
*Transaction ID: Initiated by master
*P-192 Public Key
Debug Key(X): 0x 15 20 70 09 98 44 21 a6 58 6f 9f c3 fe 7e 43 29 d2 6
*Debug Key(Y): 0x b0 9d 42 b8 1b c5 bd 00 9f 79 e4 b5 9d bb aa 85 7
BINARY
RADIX
PANE
CHAR

Figure 6 - Encapsulated Payload Message from a *Bluetooth* Device in SSP Debug Mode

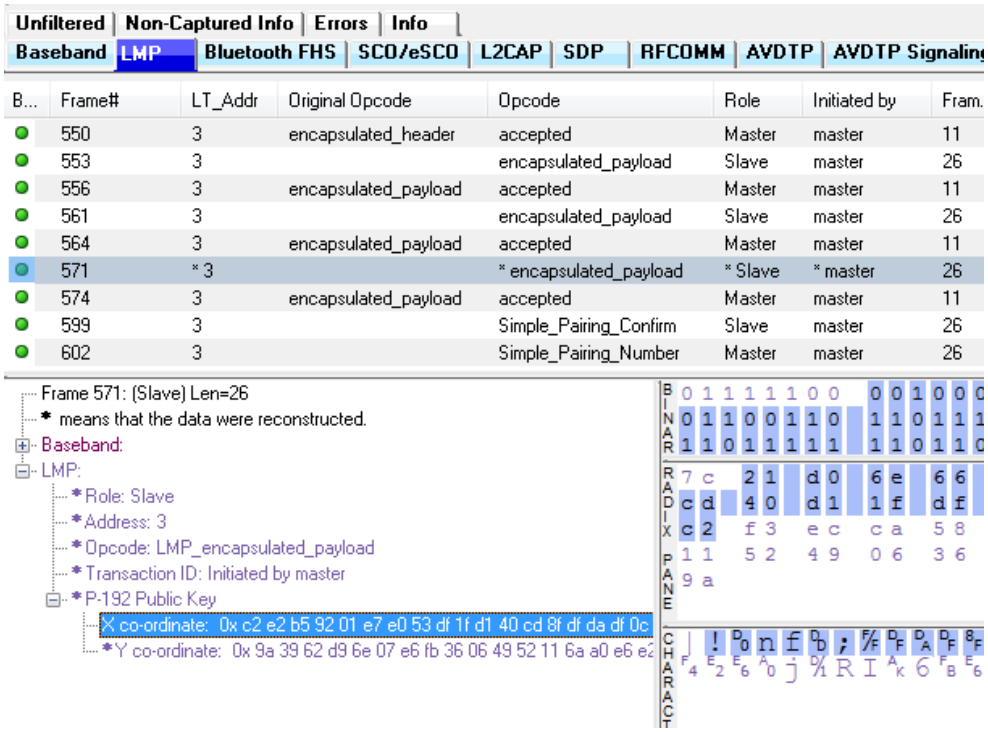


Figure 7 - Encapsulated Payload Message from a *Bluetooth* Device NOT in SSP Debug Mode

Author: Sean Clinchy

Publish Date: February 2014

A.3 Decrypting Encrypted Bluetooth® low energy

A.3.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

A.3.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.
2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
3. In this phase each device may distribute to the other device up to three keys:
    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,
    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and
    c. the Identity Resolving Key (IRK) used to generate a private address.

    Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the "keys" identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.

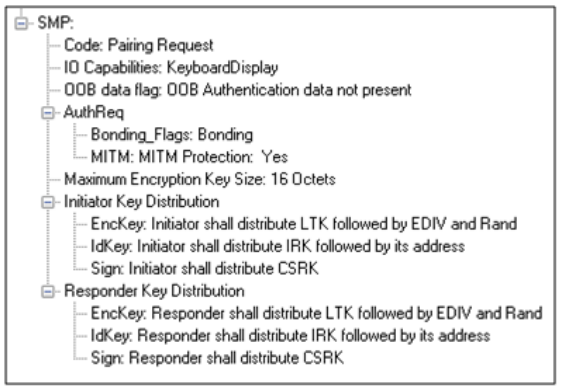

SMP:
Code: Pairing Request
IO Capabilities: KeyboardDisplay
OOB data flag: OOB Authentication data not present
AuthReq
Bonding_Flags: Bonding
MITM: MITM Protection: Yes
Maximum Encryption Key Size: 16 Octets
Initiator Key Distribution
EncKey: Initiator shall distribute LTK followed by EDIV and Rand
IdKey: Initiator shall distribute IRK followed by its address
Sign: Initiator shall distribute CSRK
Responder Key Distribution
EncKey: Responder shall distribute LTK followed by EDIV and Rand
IdKey: Responder shall distribute IRK followed by its address
Sign: Responder shall distribute CSRK

Figure 8 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

A.3.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

$$TK = \begin{cases} 6 \text{ numeric digits, Input = Keyboard} \\ 6 \text{ random digits, Input = Display} \end{cases}$$

Figure 9 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

[1]A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.

Figure 10 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

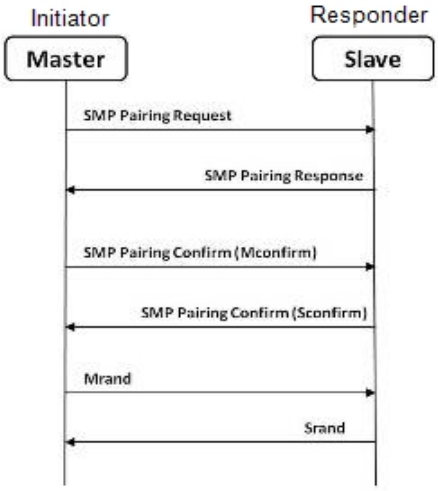


Figure 11 - Message Sequence Chart: SMP Pairing

The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

A.3.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

A.3.5 Encryption Key Generation and Distribution

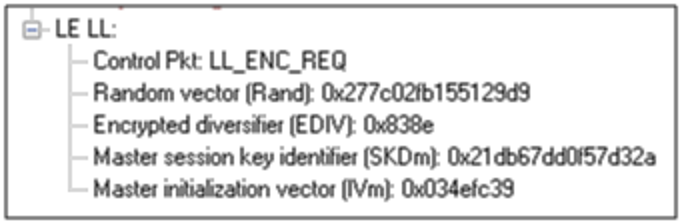

LE LL:
Control Pkt: LL_ENC_REQ
Random vector (Rand): 0x277c02fb155129d9
Encrypted diversifier (EDIV): 0x838e
Master session key identifier (SKDm): 0x21db67dd0f57d32a
Master initialization vector (IVm): 0x034efc39

Figure 12 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.

LE LL:
Control Pkt: LL_ENC_RSP
Slave session key identifier (SKDs): 0xc28aa3a44187892e
Slave initialization vector (IVs): 0x547d2236

Figure 13 - Encryption Response from Slave, Example
(ComProbe Frame Display, BPA 600 low energy capture)

A.3.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ENC_REQ) that contains the SKD_{master}. The SKD_{master} is generated using the LTK. The slave receives SKD_{master}, generates SKD_{slave}, and generates SK by concatenating parts of SKD_{master} and SKD_{slave}. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD_{slave}; the master will create the same SK.

Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master's encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

A.3.7 Decrypting Encrypted Data Using ComProbe BPA 600 low energy Capture

Note: The following discussion uses the ComProbe BPA 600 in low energy capture mode to illustrate how to identify the encryption process and to view decrypted data. However any of the ComProbe devices (BPA 500, BPA low energy) that are low energy capable will accomplish the same objectives, although the datasource setup will be slightly different for each device.

A.3.7.1 Setting up the BPA 600

1. Run the ComProbe Protocol Analysis Software and select **Bluetooth Classic/low energy (BPA 600)**. This will bring up the **BPA 600 datasource** window. This is where the parameters are set for sniffing, including the devices to be sniffed and how the link is to be decrypted.
2. Select **Devices Under Test** tab on the Datasource window.
3. Click/select **LE Only**.
4. To decrypt encrypted data transmissions between the *Bluetooth* low energy devices the ComProbe analyzer needs to know the LTK because this is the shared secret used to encrypt the session. There are two ways to provide this information and which to select will depend on the pairing method: **Just Works** or **Passkey Entry**.

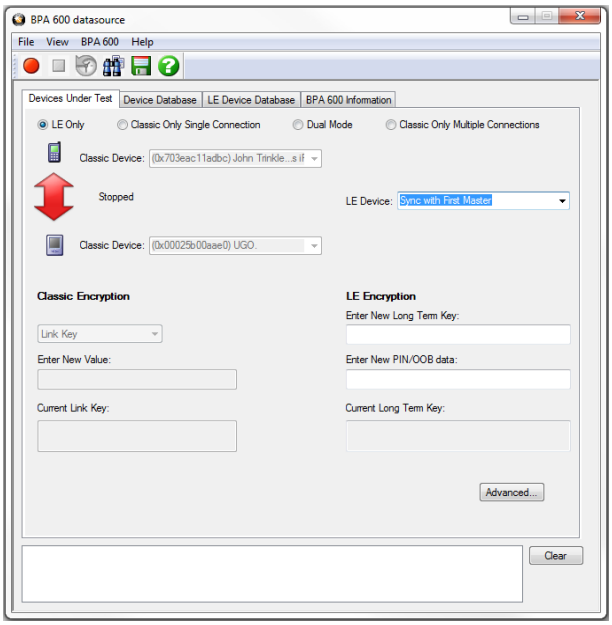


Figure 14 - ComProbe BPA 600 low energy only datasource settings

   a. **Passkey Entry** is easiest if you have the code that was displayed or entered during device pairing. The code is what is used to generate the LTK. Under **LE Encryption** enter the code in the **Enter New PIN/OOB** data text box.

   b. **Just Works** is more of a challenge because you must know the LTK that is created at the time of pairing and identification of an encrypted link.

      - If your device was previously used in an encrypted capture session, the device information including LTK can be found in the **Device Database** tab.
      - In a design and development environment the LTK is often known beforehand.
      - Capture of Host Controller Interface (HCI) events using ComProbe HSU can reveal the LTK, which is contained in the HCI_Link_Key_Request_Reply command. HCI capture is through direct connection to the device host controller. The information obtained in a direct connection can later be used in a wireless encrypted capture session that requires prior knowledge of encryption keys.

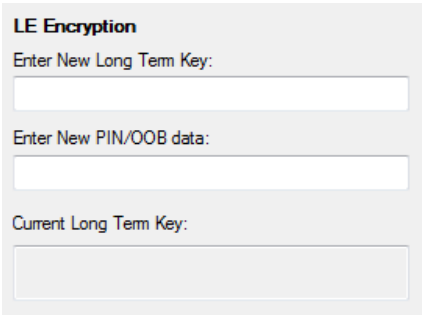


Figure 15 - BPA 600 datasource Encryption Key Entry

5. To start capture click on the Start Sniffing button on the **BPA 600 datasource** toolbar.

A.3.7.2 Use Frame Display to View Encryption/Decryption Process

A.3.7.2.1 Security Manager Protocol

The Security Manager Protocol (SMP) controls the process for pairing and key distribution. The results of a pairing and key distribution can be observed in the ComProbe software **Frame Display**. Activate the **Frame Display** by clicking on the icon on the **Control** window toolbar. On the **Frame Display** low energy protocols are shown in light green tabs. Click on the **SMP** protocol tab that will show only the SMP commands from the full data set.

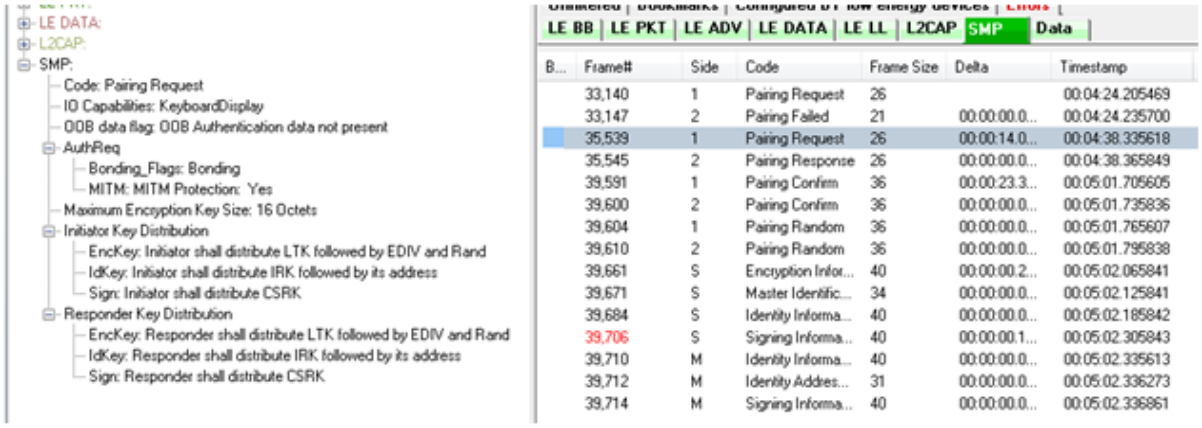

LE DATA:
L2CAP:
SMP:
Code: Pairing Request
IO Capabilities: KeyboardDisplay
OOB data flag: OOB Authentication data not present
AuthReq
Bonding_Flags: Bonding
MITM: MITM Protection: Yes
Maximum Encryption Key Size: 16 Octets
Initiator Key Distribution
EncKey: Initiator shall distribute LTK followed by EDIV and Rand
IdKey: Initiator shall distribute IRK followed by its address
Sign: Initiator shall distribute CSRK
Responder Key Distribution
EncKey: Responder shall distribute LTK followed by EDIV and Rand
IdKey: Responder shall distribute IRK followed by its address
Sign: Responder shall distribute CSRK
LE BB | LE PKT | LE ADV | LE DATA | LE LL | L2CAP | SMP | Data
B... Frame# Side Code Frame Size Delta Timestamp
33,140 1 Pairing Request 26 00:04:24.205469
33,147 2 Pairing Failed 21 00:00:00.0... 00:04:24.235700
35,539 1 Pairing Request 26 00:00:14.0... 00:04:38.335618
35,545 2 Pairing Response 26 00:00:00.0... 00:04:38.365849
39,591 1 Pairing Confirm 36 00:00:23.3... 00:05:01.705605
39,600 2 Pairing Confirm 36 00:00:00.0... 00:05:01.735836
39,604 1 Pairing Random 36 00:00:00.0... 00:05:01.765607
39,610 2 Pairing Random 36 00:00:00.0... 00:05:01.795838
39,661 S Encryption Infor... 40 00:00:00.2... 00:05:02.065841
39,671 S Master Identific... 34 00:00:00.0... 00:05:02.125841
39,684 S Identity Informa... 40 00:00:00.0... 00:05:02.185842
39,706 S Signing Informa... 40 00:00:00.1... 00:05:02.305843
39,710 M Identity Informa... 40 00:00:00.0... 00:05:02.335613
39,712 M Identity Addres... 31 00:00:00.0... 00:05:02.336273
39,714 M Signing Informa... 40 00:00:00.0... 00:05:02.336861

Figure 16 - SMP Pairing Request (Frame# 35,539) from Initiator (Side 1)

On the left side of the figure above is the **Frame Display Decode**r pane that shows the decoded information supplied in the selected frame in the Summary pane, Frame# 35,539. Shown is the SMP data associated with and encrypted link (MITM Protection = Yes). The requested keys are also shown. Selecting Frame# 35,545 would provide the response from the responder (Side 2) and would contain similar information.

Selecting Frame# 39,591 will display the Pairing Confirm from the initiator (Side 1) in the **Decoder** pane. The Confirm Value shown is the Mconfirm 128-bit random number that contains TK, Pairing Request command, Pairing Response command, initiating device address, and the responding device address. Selecting Frame# 39,600 would provide the Sconfirm random number from the responder (Side 2) with similar information from that device but the random number would be different than Mconfirm.

Once pairing is complete and an encrypted session established, the keys are distributed by the master and slave now identified by Side = M and Side = S respectively in the **Summary** pane. In Frame# 39,661 the slave has distributed LTK to the master to allow exchange of encrypted data. Frame# 39,661 through 39,714 in the Summary pane SMP tab are the key distribution frames.

Figure 17 - SMP Pairing Confirm (Frame# 39,591) from Initiator (Side 1)

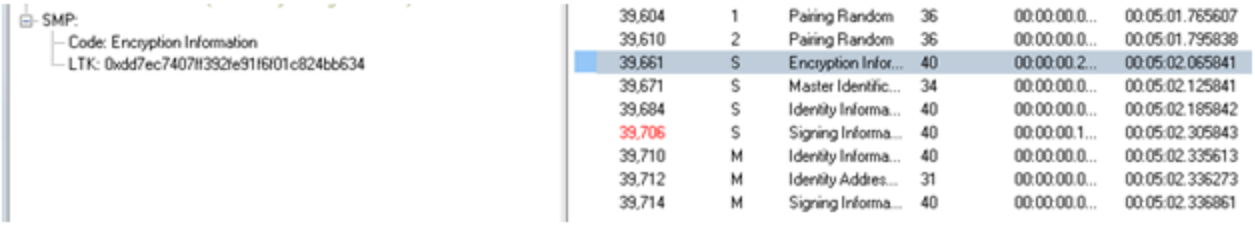


Figure 18 - SMP Key Distribution Frames

A.3.7.2.2 Link Layer

The Link Layer (LL) protocol manages the *Bluetooth* low energy radio transmissions and is involved in starting link encryption. To observe the decoded LL commands, click on the **Frame Display LE LL** tab, search for and select ControlPkt "LL_ENC_REQ". This command should originate with Side 1, the initiator of the encryption link. In Figure 11 Frame# 39,617 is selected in the Summary pane and we see the decoded LE LL frame is display in the **Decoder** pane. Shown in this frame packet is the SKDm that is the Master Session Key Diversifier (SKDmaster). In Frame# 39,623 you will find SKDslave that is combined with SKDmaster to create the Session Key (SK). Both SDKs were created using the LTK. Frame# 39,635 through 39,649 in the **LE LL** tab completes starting of the encryption process. After the slave sends LL_START_ENC_RSP (Frame# 36,649) the *Bluetooth* devices can exchange encrypted data, and the ComProbe sniffing device can also receive and decrypt the encrypted data because the appropriate "key" is provided in the **BPA 600 Datasource** window.

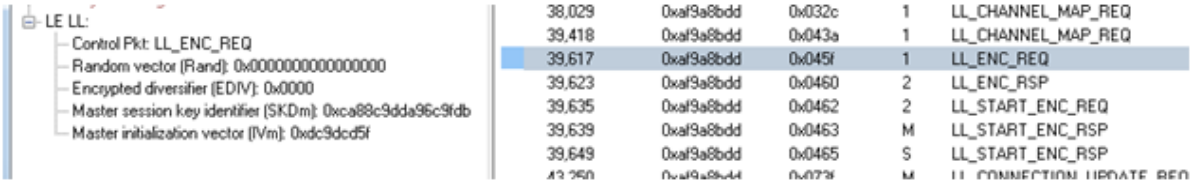

LE LL:
Control Pkt: LL_ENC_REQ
Random vector (Rand): 0x0000000000000000
Encrypted diversifier (EDIV): 0x0000
Master session key identifier (SKDm): 0xca88c9dda96c9fdb
Master initialization vector (IVm): 0xdc9dcd5f
38,029 0xaf9a8bdd 0x032c 1 LL_CHANNEL_MAP_REQ
39,418 0xaf9a8bdd 0x043a 1 LL_CHANNEL_MAP_REQ
39,617 0xaf9a8bdd 0x045f 1 LL_ENC_REQ
39,623 0xaf9a8bdd 0x0460 2 LL_ENC_RSP
39,635 0xaf9a8bdd 0x0462 2 LL_START_ENC_REQ
39,639 0xaf9a8bdd 0x0463 M LL_START_ENC_RSP
39,649 0xaf9a8bdd 0x0465 S LL_START_ENC_RSP

Figure 19 - LE LL Tab Encryption Request (Frame# 39,617) from Initiator (Side 1)

A.3.7.3 Viewing Encryption in the Message Sequence Chart

The ComProbe software **Message Sequence Chart** (**MSC**) links directly to frames being viewed in the Frame Display. Similarly MSC will display the same information as the **Frame Display Decoder** pane. Frames are synchronized between the **Frame Display Summary** pane and the **MSC**, so clicking on a frame in either window will select that same frame in the other window. Also the protocol tabs are the same in each window. To see the pairing process, click on the SMP tab.

In the image above we see Frame# 35,539 initiating the pairing from the master device. The response, SMP_Pairing Response, is sent from the slave in Frame# 35,545. SMP_Pairing Confirm occurs

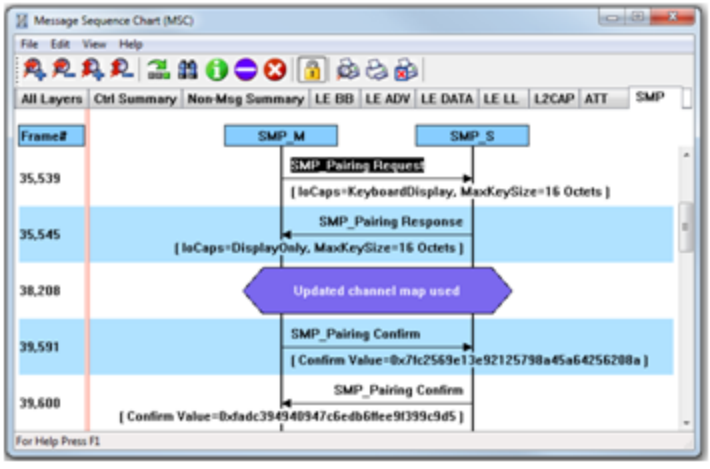


Figure 20 - MSC SMP Paring (BPA 600 low energy capture)

between the master and the slave devices at Frame# 39,591 and 39,600 respectively.

Clicking on the **MSC** LE LL tab will show the process of encrypting a session link. Clicking on Frame# 39,617 displays the LL_ENC_REQ command from the master to the slave. In the **MSC** below this command you will see the data transferred that includes SKD_{master} used to generate the LTK. At Frame# 39,623 the slave responds with LL_ENC_RSP sending SKD_{slave} to generate LTK at the master. Up to this point all transmissions are unencrypted. For this example the slave sends the request to start encryption, LL_START_ENC_REQ, at Frame#39,635. The master responds with LL_START_ENC_RSP at Frame# 39,639, and finally the slave responds with LL_START_ENC_RSP at Frame# 36,649. At this point the session link is encrypted.

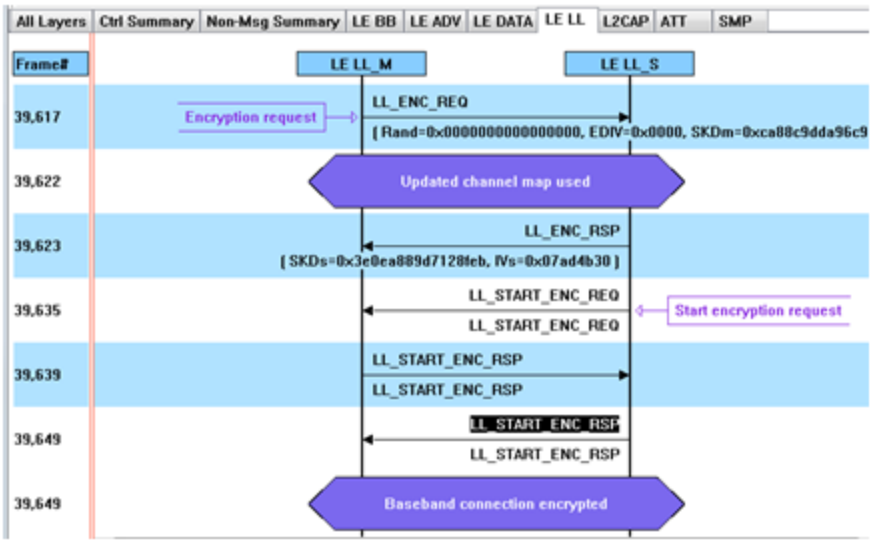


Figure 21 - MSC link Layer Encryption (BPA 600 low energy capture)

A.3.7.4 Viewing Decrypted Data

In the ComProbe software **Frame Display** click on the **LE BB** tab. Search in the **Summary** pane for Decryption Initiated = Yes frames. In the example depicted in the following figure, Frame# 39723 is selected. In the **Decoder** pane LE BB shows that the decryption was initiated and decryption was successful. In LE Data we see the Encrypted MIC value. The MIC value is used to authenticate the sender of the data packet to ensure that the data was sent by a peer device in the link and not by a third party attacker. The actual decrypted data appears between the Payload Length and the MIC in the packet. This is shown in the **Binary** pane below the **Summary** pane.

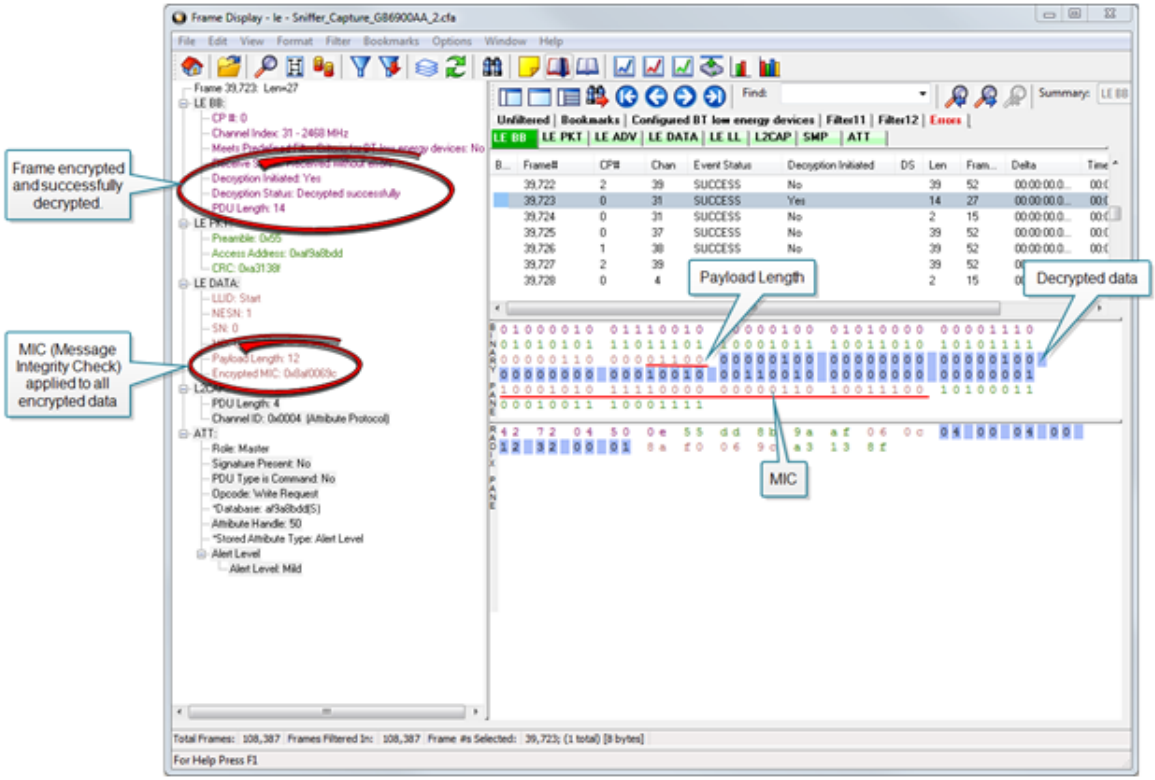


Figure 22 - Decrypted Data Example (Frame# 39,723)

Author: John Trinkle

Publish Date: 9 April 2014

Revised: 23 May 2014

A.4 Bluetooth® low energy Security

"Paris is quiet and the good citizens are content." Upon seizing power in 1799 Napoleon sent this message on Claude Chappe's optical telegraph. Chappe had invented a means of sending messages line-of-sight . The stations were placed approximately six miles apart and each station had a signaling device made of paddles on the ends of a rotating "regulator" arm whose positions represented code numbers. Each station was also outfitted with two telescopes for viewing the other stations in the link, and clocks were used to synchronize the stations. By 1803 a communications network extended from Paris across the countryside and into Belgium and Italy.

Figure 23 - Chappe's Optical Telegraph

Chappe developed several coding schemes through the next few years. The station operators only knew the codes, not what characters they represented. Not only was Chappe's telegraph system the first working network with protocols, synchronization of serial transmissions but it also used data encryption. Although cryptography has been around for millenniums—dating back to 2000 B.C. — Chappe, was the first to use it in a wide area network in the modern sense.

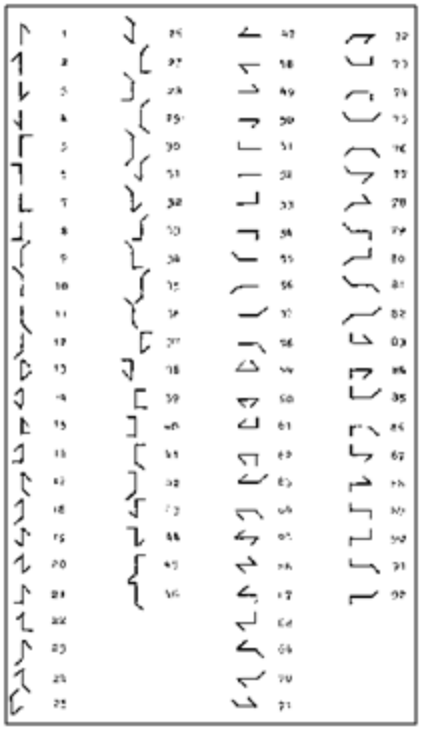


Figure 24 - Chappe's Telegraph Code

Of course anyone positioned between the telegraph stations that had Chappe's telegraph code in hand could decode the transmission. So securing the code was of paramount importance in Chappe's protocol.

Modern wireless networks such as *Bluetooth* low energy employ security measures to prevent similar potentially man-in-the-middle attacks that may have malicious intent.

Bluetooth low energy devices connected in a link can pass sensitive data by setting up a secure encrypted link. The process is similar to but not identical to *Bluetooth* BR/EDR Secure Simple Pairing. One difference is that in *Bluetooth* low energy the confidential payload includes a Message Identification Code (MIC) that is encrypted with the data. In *Bluetooth* BR/EDR only the data is encrypted. Also in Bluetooth low energy the secure link is more vulnerable to passive eavesdropping, however because of the short transmission periods this vulnerability is considered a low risk. The similarity to BR/EDR occurs with "shared secret key", a fundamental building block of modern wireless network security.

This paper describes the process of establishing a *Bluetooth* low energy secure link.

A.4.1 How Encryption Works in *Bluetooth* low energy

Data encryption is used to prevent passive and active—man-in-the-middle (MITM) — eavesdropping attacks on a *Bluetooth* low energy link. Encryption is the means to make the data unintelligible to all but the *Bluetooth* master and slave devices forming a link. Eavesdropping attacks are directed on the over-the-air transmissions between the *Bluetooth* low energy devices, so data encryption is accomplished prior to transmission using a shared, secret key.

A.4.2 Pairing

A *Bluetooth* low energy device that wants to share secure data with another device must first pair with that device. The Security Manager Protocol (SMP) carries out the pairing in three phases.

1. The two connected *Bluetooth* low energy devices announce their input and output capabilities and from that information determine a suitable method for phase 2.
2. The purpose of this phase is to generate the Short Term Key (STK) used in the third phase to secure key distribution. The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
3. In this phase each device may distribute to the other device up to three keys:
    a. the Long Term Key (LTK) used for Link Layer encryption and authentication,
    b. the Connection Signature Resolving Key (CSRK) used for data signing at the ATT layer, and

c. the Identity Resolving Key (IRK) used to generate a private address.

Of primary interest in this paper is the LTK. CSRK and IRK are covered briefly at the end.

Bluetooth low energy uses the same pairing process as Classic *Bluetooth*: Secure Simple Pairing (SSP). During SSP initially each device determines its capability for input and output (IO). The input can be None, Yes/No, or Keyboard with Keyboard having the ability to input a number. The output can be either None or Display with Display having the ability to display a 6-digit number. For each device in a paring link the IO capability determines their ability to create encryption shared secret keys.

The Pairing Request message is transmitted from the initiator containing the IO capabilities, authentication data availability, authentication requirements, key size requirements, and other data. A Pairing Response message is transmitted from the responder and contains much of the same information as the initiators Pairing Request message thus confirming that a pairing is successfully negotiated.

In the sample SMP decode, in the figure at the right, note the "keys" identified. Creating a shared, secret key is an evolutionary process that involves several intermediary keys. The resulting keys include,

1. IRK: 128-bit key used to generate and resolve random address.
2. CSRK: 128-bit key used to sign data and verify signatures on the receiving device.
3. LTK: 128-bit key used to generate the session key for an encrypted connection.
4. Encrypted Diversifier (EDIV): 16-bit stored value used to identify the LTK. A new EDIV is generated each time a new LTK is distributed.
5. Random Number (RAND): 64-bit stored value used to identify the LTK. A new RAND is generated each time a unique LTK is distributed.

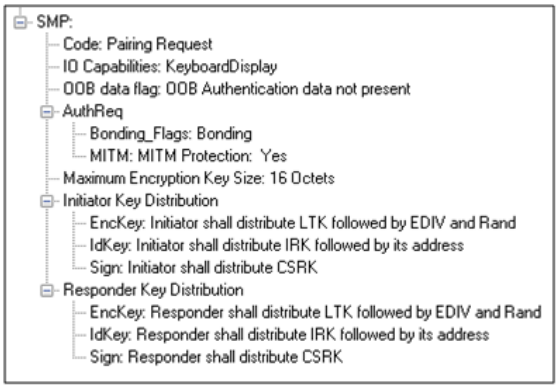

SMP:
Code: Pairing Request
IO Capabilities: KeyboardDisplay
OOB data flag: OOB Authentication data not present
AuthReq
Bonding_Flags: Bonding
MITM: MITM Protection: Yes
Maximum Encryption Key Size: 16 Octets
Initiator Key Distribution
EncKey: Initiator shall distribute LTK followed by EDIV and Rand
IdKey: Initiator shall distribute IRK followed by its address
Sign: Initiator shall distribute CSRK
Responder Key Distribution
EncKey: Responder shall distribute LTK followed by EDIV and Rand
IdKey: Responder shall distribute IRK followed by its address
Sign: Responder shall distribute CSRK

Figure 25 - Sample Initiator Pairing Request Decode (ComProbe Frame Display, BPA 600 low energy capture)

Of particular importance to decrypting the encrypted data on a *Bluetooth* low energy link is LTK, EDIV, and RAND.

A.4.3 Pairing Methods

The two devices in the link use the IO capabilities from Pairing Request and Pairing Response packet data to determine which of two pairing methods to use for generation of the Temporary Key (TK). The two methods are **Just Works** and **Passkey Entry**[1]. An example of when **Just Works** method is appropriate is when the IO capability input = None and output = None. An example of when Passkey Entry would be appropriate would be if input= Keyboard and output = Display. There are 25 combinations that result in 13 **Just Works** methods and 12 **Passkey Entry** methods.

In **Just Works** the TK = 0. In the **Passkey Entry** method,

$$TK = \begin{cases} 6 \text{ numeric digits, Input = Keyboard} \\ 6 \text{ random digits, Input = Display} \end{cases}$$

[1]A third method, Out Of Band (OOB), performs the same as **Pass Key**, but through another external link such as NFC.

Figure 26 - Initiator Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

Figure 27 - Responder Pairing Confirm Example (ComProbe Frame Display, BPA 600 low energy capture)

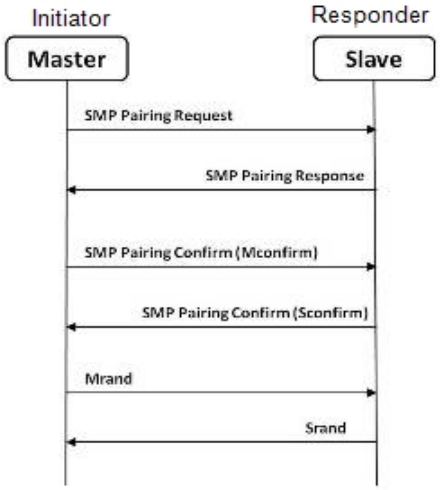


Figure 28 - Message Sequence Chart: SMP Pairing

The initiating device will generate a 128-bit random number that is combined with TK, the Pairing Request command, the Pairing Response command, the initiating device address and address type, and the responding device address and address type. The resulting value is a random number **Mconfirm** that is sent to the responding device by the Pairing Confirm command. The responding device will validate the responding device data in the Pairing Confirm command and if it is correct will generate a **Sconfirm** value using the same methods as used to generate **Mconfirm** only with different 128-bit random number and TK. The responding device will send a Pairing Confirm command to the initiator and if accepted the authentication process is complete. The random number in the **Mconfirm** and **Sconfirm** data is **Mrand** and **Srand** respectively. **Mrand** and **Srand** have a key role in setting encrypting the link.

Finally the master and slave devices exchange **Mrand** and **Srand** so that the slave can calculate and verify Mconfirm and the master can likewise calculate and verify Sconfirm.

A.4.4 Encrypting the Link

The Short Term Key (STK) is used for encrypting the link the first time the two devices pair. STK remains in each device on the link and is not transmitted between devices. STK is formed by combining **Mrand** and **Srand** which were formed using device information and TKs exchanged with Pairing Confirmation (**Pairing Confirm**).

A.4.5 Encryption Key Generation and Distribution

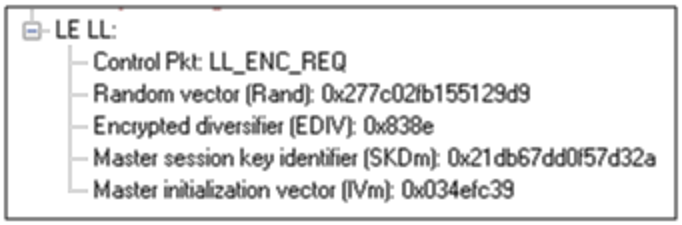

LE LL:
Control Pkt: LL_ENC_REQ
Random vector (Rand): 0x277c02fb155129d9
Encrypted diversifier (EDIV): 0x838e
Master session key identifier (SKDm): 0x21db67dd0f57d32a
Master initialization vector (IVm): 0x034efc39

Figure 29 - Encryption Request from Master, Example (ComProbe Frame Display, BPA 600 low energy capture

To distribute the LTK, EDIV, and Rand values an encrypted session needs to be set up. The initiator will use STK to enable encryption on the link. Once an encrypted link is set up, the LTK is distributed. LTK is a 128-bit random number that the slave device will generate along with EDIV and Rand. Both the master and slave devices can distribute these numbers, but *Bluetooth* low energy is designed to conserve energy, so the slave device is often resource constrained and

does not have the database storage resources for holding LTKs. Therefore the slave will distribute LTK, EDIV, and Rand to the master device for storage. When a slave begins a new encrypted session with a previously linked master device, it will request distribution of EDIV and Rand and will regenerate LTK.

LE LL:
Control Pkt: LL_ENC_RSP
Slave session key identifier (SKDs): 0xc28aa3a44187892e
Slave initialization vector (IVs): 0x547d2236

Figure 30 - Encryption Response from Slave, Example
(ComProbe Frame Display, BPA 600 low energy capture)

A.4.6 Encrypting The Data Transmission

Data encryption begins with encrypting the link. The Session Key (SK) is created using a session key diversifier (SKD). The first step in creating a SK is for the master device to send Link Layer encryption request message (LL_ENC_REQ) that contains the SKD_{master}. The SKD_{master} is generated using the LTK. The slave receives SKD_{master}, generates SKD_{slave}, and generates SK by concatenating parts of SKD_{master} and SKD_{slave}. The slave device responds with an encryption response message (LL_ENC_RSP) that contains SKD_{slave}; the master will create the same SK.

Now that a SK has been calculated, the master and slave devices will now begin a handshake process. The slave will transmit unencrypted LL_START_ENC_REQ, but sets the slave to receive encrypted data using the recently calculated SK. The master responds with encrypted LL_START_ENC_RSP that uses the same SK just calculated and setting the master to receive encrypted data. Once the slave receives the master's encrypted LL_START_ENC_RSP message and responds with an encrypted LL_START_ENC_RSP message the *Bluetooth* low energy devices can now begin transmitting and receiving encrypted data.

A.4.7 IRK and CSRK Revisited

Earlier in this paper it was stated that LTK would be the focus, however the IRK and CSRK were mentioned. We revisit these keys because they are used in situations that require a lesser level of security. First let us note that IRK and CSRK are passed in an encrypted link along with LTK and EDIV.

Use of the IRK and CSRK attempt to place an identity on devices operating in a piconet. The probability that two devices will have the same IRK and generate the same random number is low, but not absolute.

IRK and *Bluetooth* low energy Privacy Feature

Bluetooth low energy has a feature that reduces the ability of an attacker to track a device over a long period buy frequently and randomly changing an advertising device's address. This is the privacy feature. This feature is not used in the discovery mode and procedures but is used in the connection mode and procedures.

If the advertising device was previously discovered and has returned to an advertising state, the device must be identifiable by trusted devices in future connections without going through discovery procedure again. The IRK stored in the trusted device will overcome the problem of maintaining privacy while saving discovery computational load and connection time. The advertising devices IRK was passed to the master device during initial bonding. The a master device will use the IRK to identify the advertiser as a trusted device.

CSRK and Signing for Authentication

Bluetooth low energy supports the ability to authenticate data sent over an unencrypted ATT bearer between two devices in a trust relationship. If authenticated pairing has occurred and encryption is not required (security mode 2) data signing is used if CSRK has been exchanged. The sending device attaches a digital signature after the data in

the packet that includes a counter and a message authentication code (MAC). The key used to generate MAC is CSRK. Each peer device in a piconet will have a unique CSRK.

The receiving device will authenticate the message from the trusted sending device using the CSRK exchanged from the sending device. The counter is initialized to zero when the CSRK is generated and is incremented with each message signed with a given CSRK. The combination of the CSRK and counter mitigates replay attacks.

A.4.8 Table of Acronyms

CSRK	Connection Signature Resolving Key
EDIV	Encrypted Diversifier
IO	Input and output
IRK	Identity Resolving Key
LTK	Long Term Key
Mconfirm	128-bit confirm value from initiator
MIC	Message Integrity Check
MITM	Man-in-the-middle
Mrand	128-bit random number used to generate Mconfirm
OOB	Out of Band
RAND	Random Number
Sconfirm	128-bit confirmation value from the responder
SK	Session key
SMP	Security Manager Protocol
Srand	128-bit random number used to generate Sconfirm
SSP	Secure Simple Pairing
STK	Short Term Key
TK	Temporary Key

Author: John Trinkle

Publish Date:21 May 2014

A.5 Bluetooth Virtual Sniffing

A.5.1 Introduction

The ComProbe software Virtual sniffing function simplifiesBluetooth® development and is easy to use. Frontline's Virtual sniffing with Live Import provides the developer with an open interface from any application to ComProbe software so that data can be analyzed and processed independent of sniffing hardware. Virtual sniffing can also add value to other *Bluetooth* development tools such as *Bluetooth* stack SDKs (Software Development Kits) and *Bluetooth* chip development kits.

This white paper discusses:

- Why HCI sniffing and Virtual sniffing are useful.
- *Bluetooth* sniffing history.
- What is Virtual sniffing?
- Why Virtual sniffing is convenient and reliable.
- How Virtual sniffing works.
- Virtual sniffing and Bluetooth stack vendors.
- Case studies: Virtual sniffing and Bluetooth mobile phone makers.
- Virtual sniffing and you. • Where to go for more information.

A.5.2 Why HCI Sniffing and Virtual Sniffing are Useful

Because the *Bluetooth* protocol stack is very complex, a *Bluetooth* protocol analyzer is an important part of all *Bluetooth* development environments. The typical *Bluetooth* protocol analyzer "taps" a *Bluetooth* link by capturing data over the air. For many *Bluetooth* developers sniffing the link between a *Bluetooth* Host CPU and a *Bluetooth* Host Controller—also known as HCI-sniffing—is much more useful than air sniffing.

HCI-sniffing provides direct visibility into the commands being sent to a *Bluetooth* chip and the responses to those commands. With air sniffing a software engineer working on the host side of a Bluetooth chip has to infer and often guess at what their software is doing. With HCI-sniffing, the software engineer can see exactly what is going on. HCI-sniffing often results in faster and easier debugging than air sniffing.

ComProbe software's Virtual sniffing feature is a simple and easy way to perform HCI-sniffing. Virtual sniffing is not limited to just HCI-sniffing, but it is the most common use and this white paper will focus on the HCI-sniffing application of Virtual sniffing.

It is also important to understand that ComProbe software is a multi-mode product. ComProbe software does support traditional air sniffing. It also supports serial HCI sniffing (for the H4 (HCI UART), H5 (3-wire UART) , and BCSP (BlueCore Serial Protocol) protocols), USB HCI (H2) sniffing, SDIO sniffing, and Virtual sniffing. So with ComProbe software nothing is sacrificed—the product is simply more functional than other Bluetooth protocol analyzers.

A.5.3 *Bluetooth* Sniffing History

Frontline has a strong appreciation for the importance of HCI sniffing because of the way we got involved with *Bluetooth*. Because of our company history, we are uniquely qualified to offer a multi-mode analyzer that provides many ways to sniff and supports a wide variety of protocols. This brief *Bluetooth* sniffing history should help you understand our approach to *Bluetooth* protocol analysis.

In the early days of *Bluetooth*, there were no commercially available *Bluetooth* protocol analyzers, so developers built their own debug tools and/or used protocol analyzers that weren't built for *Bluetooth*. Many developers built homegrown HCI analyzers—basically hex dumps and crude traces—because they recognized the need for visibility into the HCI interface and because it was too difficult to build air sniffers. Several companies developed air sniffers because they saw a market need and because they realized that they could charge a high price (USD $25,000 and higher).

Two *Bluetooth* chip companies, Silicon Wave and Broadcom were using Frontline's Serialtest® serial analyzer to capture serial HCI traffic and then they would manually decode the HCI byte stream. This manual decoding was far too much work and so, independently, Silicon Wave and Broadcom each requested that Frontline produce a serial HCI *Bluetooth* analyzer that would have all the features of Serialtest. In response to these requests Frontline developed SerialBlue®—the world's first commercially available serial HCI analyzer.

The response to SerialBlue was very positive. When we asked our *Bluetooth* customers what they wanted next we quickly learned that there was a need for an affordable air sniffer that provided the same quality as SerialBlue. We also learned that the ultimate *Bluetooth* analyzer would be one that sniff air and sniff HCI simultaneously.

As work was progressing on our combination air sniffer and HCI sniffer the functional requirements for *Bluetooth* analyzers were changing. It was no longer good enough just to decode the core *Bluetooth* protocols (LMP, HCI, L2CAP, RFCOMM, and OBEX). Applications were beginning to be built on top of *Bluetooth* and therefore application level protocol decoding was becoming a requirement. For example, people were starting to browse the Internet using *Bluetooth*-enabled phones and PDAs therefore a good *Bluetooth* analyzer would need to support TCP/IP, HTTP, hands-free, A2DP, etc.

For Frontline to support for these higher levels protocols was no problem since they were already in use in other Frontline analyzer products. People have been using Frontline Serialtest serial analyzers and Ethertest™ Ethernet analyzer to troubleshoot TCP/IP and Internet problems for many years.

As we continued to work closely with the *Bluetooth* community we also came across one other requirement: sniffing itself had to be made easier. We took a two-pronged approach to this problem. We simplified air sniffing (and we continue to work on simplifying the process of air sniffing) and we invented Virtual sniffing.

A.5.4 Virtual Sniffing—What is it?

Historically, protocol analyzers have physically tapped the circuit being sniffed. For example, an Ethernet circuit is tapped by plugging into the network. A serial connection is sniffed by passively bridging the serial link. A *Bluetooth* air sniffer taps the piconet by synchronizing its clock to the clock of the piconet Master.

Not only is there a physical tap in traditional sniffing, but the sniffer must have some knowledge of the physical characteristics of the link being sniffed. For example, a *Bluetooth* air sniffer must know the BD_ADDR of at least one piconet member to allow it perform clock synchronization. A serial sniffer must know the bit rate of the tapped circuit or be physically connected to the clock line of the circuit.

With Virtual sniffing the protocol analyzer itself does not actually tap the link and the protocol analyzer does not require any knowledge of the physical characteristics of the link.

In computer jargon, “virtual” means “not real”. Virtual memory is memory that doesn’t actually exist. Virtual reality is something that looks and feels real, but isn’t real. So we use the term Virtual sniffing, because there is sniffing taking place, but not in the traditional physical sense.

A.5.5 The Convenience and Reliability of Virtual Sniffing

Virtual sniffing is the most convenient and reliable form of sniffing and should be used in preference to all other forms of sniffing whenever practical. Virtual sniffing is convenient because it requires no setup to use except for a very small amount of software engineering (typically between one and four hours) that is done once and then never again. Once support for Virtual sniffing has been built into application or into a development environment none of the traditional sniffing setup work need be done.

This means:

- NO piconet synchronization.
- NO serial connection to tap.
- NO USB connection to tap.

Virtual sniffing is reliable because there is nothing that can fail. With Virtual sniffing all data is always captured.

A.5.6 How Virtual Sniffing Works

ComProbe software Virtual sniffing works using a feature called Live Import. Any application can feed data into ComProbe software using Live Import. A simple API provides four basic functions and a few other more advanced functions. The four basic Live Import functions are:

- Open a connection to ComProbe software.
- Close a connection to ComProbe software.
- Send an entire packet to ComProbe software.
- Send a single byte to ComProbe software.

All applications that send data to ComProbe software via Live Import use the first two functions. Usually only one of the two Send functions is used by a particular application. When ComProbe software receives data from the application via Live Import, the data is treated just as if it had been captured on a Frontline ComProbe sniffer. The entire protocol stack is fully decoded.

With Virtual sniffing the data can literally be coming from anywhere. ComProbe software does not care if the data being analyzed is being captured on the machine where ComProbe software is running or if the data is being captured remotely and passed into ComProbe software over an Internet connection.

A.5.7 Virtual Sniffing and *Bluetooth* Stack Vendors

As the complexity of the *Bluetooth* protocol stack increases *Bluetooth* stack vendors are realizing that their customers require the use of a powerful *Bluetooth* protocol analyzer. Even if the stack vendor’s stack is bug free,

there are interoperability issues that must be dealt with.

The homegrown hex dumps and trace tools from the early days of *Bluetooth* just are not good enough anymore. And building a good protocol analyzer is not easy. So stack vendors are partnering with Frontline. This permits the stack vendors to concentrate of improving their stack.

The typical *Bluetooth* stack vendor provides a Windows-based SDK. The stack vendor interfaces their SDK to ComProbe software by adding a very small amount of code to the SDK, somewhere in the transport area, right about in the same place that HCI data is sent to the Host Controller.

If ComProbe software is installed on the PC and the Virtual sniffer is running then the data will be captured and decoded by ComProbe software, in real-time. If ComProbe software is not installed or the Virtual sniffer is not running then no harm is done. Virtual sniffing is totally passive and has no impact on the behavior of the SDK.

One Frontline stack vendor partner feels so strongly about ComProbe software that not only have they built Virtual sniffing support in their SDK, but they have made ComProbe software an integral part of their product offering. They are actively encouraging all customers on a worldwide basis to adopt ComProbe software as their protocol analysis solution.

A.5.8 Case Studies: Virtual Sniffing and *Bluetooth* Mobile Phone Makers

Case Study # 1

A *Bluetooth* mobile phone maker had been using a homemade HCI trace tool to debug the link between the Host CPU in the phone the *Bluetooth* chip. They also were using an air sniffer. They replaced their entire sniffing setup by moving to ComProbe software.

In the original test setup the Host CPU in the phone would send debug messages and HCI data over a serial link. A program running on a PC logged the output from the Host CPU. To implement the new system using Virtual sniffing, a small change was made to the PC logging program and it now sends the data to ComProbe software using the Live Import API. The HCI traffic is fully decoded and the debug messages are decoded as well.

The decoder for the debug messages was written using ComProbe software's DecoderScript feature. DecoderScript allows ComProbe software user to write custom decodes and to modify decodes supplied with ComProbe software. DecoderScript is supplied as a standard part of ComProbe software. In this case, the customer also created a custom decoder for HCI Vendor Extensions.

The air sniffer that was formerly used has been replaced by the standard ComProbe software air sniffer.

Case Study # 2

A second *Bluetooth* mobile phone maker plans to use Virtual sniffing in conjunction with a Linux-based custom test platform they have developed. Currently they capture serial HCI traffic on their Linux system and use a set of homegrown utilities to decode the captured data.

They plan to send the captured serial HCI traffic out of the Linux system using TCP/IP over Ethernet. Over on the PC running ComProbe software they will use a simple TCP/IP listening program to bring the data into the PC and this program will hand the data off to ComProbe software using the Live Import API.

A.5.9 Virtual Sniffing and You

If you are a *Bluetooth* stack vendor, a *Bluetooth* chip maker, or a maker of any other products where integrating your product with ComProbe software's Virtual sniffing is of interest please contact Frontline to discuss your requirements. There are numerous approaches that we can use to structure a partnership program with you. We believe that a partnership with Frontline is an easy and cost-effective way for you to add value to your product offering.

If you are end customer and you want to take advantage of Virtual sniffing, all you need to do is buy any Frontline *Bluetooth* product. Virtually sniffing comes standard with product.

Author: Eric Kaplan

Publish Date: May 2003

Revised: December 2013

Index

A

A2DP Decoder Parameters 42

Aborted Frame 227

About Display Filters 94

About L2CAP Decoder Parameters 47

Absolute Time 233

Adaptive Frequency Hopping

PER Stats 183

Add a New or Save an Existing Template 41

Adding a New Predefined Stack 62

Adding Comments To A Capture File 215

Advanced System Options 226

Apply Capture Filters 96

Apply Display Filters 94-97, 99

ASCII 71

character set 238

viewing data in 71

ASCII Codes 238

ASCII Pane 91

Auto-Sizing Column Widths 89

Automatically Request Missing Decoding Information 64

Automatically Restart 224

Automatically Restart Capturing After 'Clear Capture Buffer' 224

Automatically Save Imported Capture Files 224

Autotraversal 62, 64

AVDTP 42, 44-45

AVDTP Override Decode Information 45

Average Throughput Indicators

Average Throughput - Selected 121

Average_Throughput_Indicators 120

B

Baudot 71, 223

Baudot Codes 238

Begin Sync Character Strip 73

Binary 70, 197

Binary Pane 92

BL 240

Bluetooth Timeline 110

Bookmarks 210-211

Boolean 97, 102

BPA - Update Firmware 18

BPA 500 - Capture Data 57

BPA 500 - Classic 24, 30

BPA 500 - Hardware Settings 36

BPA 500 - low energy 21, 26

BPA 500 Advanced I/O Settings 37

BPA 500 BR/EDR IO Settings 19

BPA 500 Data Capture Methods 10

BPA 600 33

BPA Device Database 34

Broken Frame 72

BS 240

BT Snoop File Format 235

BT Timeline Legend 125

Btsnoop 235

Buffer 214, 224

Buffer Overflow 224

Buffer/File Options 224

Byte 68, 70, 92, 238

Searching 200

byte export 84

C

Calculating Data Rates and Delta Times 68
Capture Buffer 214, 224, 226
  Capture Buffer Size 224
Capture File 56, 214-217, 224, 226
  auto-save imported files 224
  capture to a series of files 224
  capture to one file 224
  changing default location of 228
  changing max size of 224, 226
  framing captured data 63
  loading 216
  reframing 63
  removing framing markers 63
  saving 214-215
  starting capture to file 56
Capturing 56
  Data to Disk 56
CFA file 215-216
Changing Default File Locations 228
Character 197, 239
  Character Pane 91
Character Set 71, 238-239
Choosing a Data Capture Method 8
Clear Capture Buffer 224
CN 240
Coexistence View 144
  le Devices Radio Buttons 158
  Legend 159
  Set Button 157
Throughput Graph 149
  Discontinuities 150
  Dots 153
  Swap Button 152
  Viewport 151
  Zoom Cursor 156
  Zoomed 154
    Freeze Y 155
    Unfreeze Y 155
    Y Scales Frozen 155
Throughput Indicators 146
Throughput Radio Buttons 158
Timeline Radio Buttons 158
Timelines 159
  discontinuities 166
  high-speed 168
  packet 159
  two timelines 164
Toolbar 144
Tooltip 150
  relocate 150, 162
Color of Data Bytes 93
Colors 93
Comma Separated File 220
Compound Display Filters 97
ComProbe BPA 500 - Classic Only Single Connection 24
Confirm CFA Changes 216
Context For Decoding 64
Control Characters 239
Control Signals 72, 230

Control Window 17, 224
Configuration Information 13
Conversation Filters 99
CPAS - Capture Data 57
CPAS Control Window Toolbar 12
CR 240
CRC 68
CSV Files 220
Custom Protocol Stack 60, 62
Custom Stack 61-62
Customizing Fields in the Summary Pane 89

D

D/1 240
D/2 239
D/3 239
D/4 239
D/E 240
Data 68, 213-214
Capturing 56
Data Byte Color Denotation 93
Data Errors 206
Data Extraction 190
Data Rates 68
Decimal 70
Decode Pane 90
decoder 241
Decoder Parameters 38
DecoderScript 241
Decodes 38, 60, 65, 74, 80, 90, 194
Default File Locations 228
Delete a Template 41
Deleting Display Filters 99
Delta Times 68
Direction 99
Directories 228
Disabling 224
Discontinuities 124
Display Filters 94, 100-102
Display Options 234
DL 240
Dots 90
Driver 241
Duplicate View 66, 68, 83-84
DUT 33

E

E/B 240
E/C 240
Easy Protocol Filtering 109
EBCDIC 71
EBCDIC Codes 239
EIR 60
EM 239
EQ 240
Errors 206, 230
ET 239
Event Display 65, 83, 221
Event Display Export 221
Event Display Toolbar 66
Event Numbering 238
Event Pane 92
Event Symbols 72
EX 239

Exclude 96
Exclude Radio Buttons 96
Expand All/Collapse All 90
Expand Decode Pane 84
Export
Export Baudot 223
Export Events 221
Export Filter Out 223
Export Payload Throughput Over Time 123
Extended Inquiry Response 60

F

F/F 239
FCSs 68
Field Width 89
File 213-216, 224
File Locations 228
File Series 224
File Types Supported 216
Filtering 108
Filters 94-97, 99-102, 109
Find 194, 197-198, 200-201, 206
Find - Bookmarks 208
Find Introduction 193
Font Size 73
Frame Display 74, 77, 80-81, 83-84, 89-93
Frame Display - Change Text Highlight Color 92
Frame Display - Find 81
Frame Display Status Bar 80
Frame Display Toolbar 77
Frame Display Window 75
Frame Recognizer Change 72
Frame Symbols 90
Frame Information on the Control Window 13
Freeze 69
FS 240
FTS Serial Driver 241

G

Go To 200
Green Dots in Summary Pane 90
GS 239

H

Hex 70
Hexadecimal 91
Hiding Display Filters 99
Hiding Protocol Layers 80
High Resolution Timestamping 233
HT 240

I

I/O Settings Change 72
Icons in Data on Event Display 72
Importable File Types 217
Importing Capture Files 216
INCLUDE 96
Include/Exclude 96

L

L2CAP 47
L2CAP Override Decode Information 48
Layer Colors 93
LF 240
Link Key 24, 26, 30, 57
LSB 26, 33, 59
Live Update 69

Logical Byte Display 81
Logical Bytes 81
Long Break 73
Low Energy Timeline
Button Bar/Legend 127
Discontinuities 139
Legend 132
Navigating and Selecting Data 140
Zooming 141
low energy Timeline Introduction 126-127
Low Power 73

M

Main Window 11
Message Sequence Chart 171
Message Sequence Chart - Find and Go To 175
Message Sequence Chart - Go To 176
Minimizing 17
Missing Bluetooth Clock 125
Missing Decode Information 44, 50
Mixed Channel/Sides 71
Mixed Sides Mode 71
Modem Lead Names 230
Modify Display Filters 101-102
Multiple Event Displays 68
Multiple Frame Displays 84

N

NK 240
Node Filters 99
Nonprintables 223
Notes 215
NU 239
Number Set 70
Numbers 238

O

Object Throughput Stats File 123
Octal 70
One_Second_Throughput_Indicators 121
Open 68
Open Capture File 216
Options 224, 226-227, 231
Other Term
Subterm 16
Override Decode Information 45, 48, 51
Overriding Frame Information 64
Overrun Errors 207

P

Packet Error Rate (PER Stats) 179
Packet Error Rate 179
PER Stats Scroll Bar 187
Packet Timeline 115, 124
Packet Timeline Menu Bar 116
Packet_Depiction 110
Packet_Navigation_and_Selection 114
Packet_Timeline_Introduction 110
Packet_Timeline_Visual_Elements 118
Panes 84
Pattern 196
Pause 56
Performance Notes 234
Printing 219
Printing from the Frame Display 217
Progress Bars 238

Protocol
Protocol Layer Colors 93
Protocol Layer Filtering 108
Protocol Stack 61-62, 64

Q

Quick Filtering 108

R

Radix 70, 91
Reframe 63
Reframing 63
Relative Time 198, 233
Remove
Bookmarks 210-211
Columns 89
Custom Stack 61
Filters 99-100
Framing Markers 63
Reset Panes 84
Resolution 232
Resumed 72
Revealing Protocol Layers 80
RFCOMM 49-51
RFCOMM Missing Decode Information 50
RFCOMM Override Decode Information 51
RS 239

S

Save 96, 213-215
Save As 213
Saving 214-215
Display Filter 95
Imported Capture Files 224
Saving the Capture File using File > Save or the Save icon 213
Search 194, 196, 198, 200-201, 206, 209-211
binary value 196
bookmarks 211
character string 196
errors 206
event number 201
frame number 200
hex pattern 196
pattern 196
special event 201
timestamp 198
wildcards 196
Seed Value 68
Serial Driver 241
Short Break 73
Side Names 230
Sides 230
Sorting Frames 81
Special Events 201
Start 72
Start Up Options 227
Summary 86
Summary Pane 86, 89-90
Sync Dropped 73
Sync Found 73
Sync Hunt Entered 73
Sync Lost 73
Synchronization 83
System Settings 224, 226

T

Technical Support 243

Test Device Began Responding 73

Test Device Stopped Responding 73

Throughput Displays

Throughput_Displays 120

Throughput Graph 122

Timestamp 210, 232-233

Timestamping 210, 231, 233

Timestamping Disabled 73

Timestamping Enabled 73

Timestamping Options 224, 231

Timestamping Resolution 232

Timestamps 231, 233

Transferring Packets 56

Truncated Frame 73

U

Underrun Error 73

Unframe 63

Unframe Function 63

Unframing 63

Unknown Event 73

V

vendor specific decoder 241

Viewing Data Events 69

W

Wrap Buffer/File 224

Z

Zooming 166

Zooming 120

zooming cursor 156